EXHIBIT 15

EXHIBIT 15

US006836549B1

(12) **United States Patent**
Quan et al.

(10) **Patent No.: US 6,836,549 B1**
(45) **Date of Patent: Dec. 28, 2004**

(54) **METHOD AND APPARATUS FOR SYNTHESIZING AND REDUCING THE EFFECTS OF VIDEO COPY PROTECTION SIGNALS**

(75) Inventors: **Ronald Quan**, Cupertino, CA (US); **Gerow D. Brill**, Danbury, CT (US)

(73) Assignee: **Macrovision Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/388,296**

(22) Filed: **Sep. 1, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/098,804, filed on Sep. 2, 1998.

(51) **Int. Cl.**[7] **H04N 7/167**

(52) **U.S. Cl.** **380/221**; 380/201; 380/203; 380/204; 380/205; 380/210; 380/224; 713/200

(58) **Field of Search** 380/201, 203–205, 380/210, 224, 22; 713/200

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,695,901	A *	9/1987	Ryan	380/204
4,697,211	A *	9/1987	Balaban et al.	348/532
4,698,679	A *	10/1987	Balaban et al.	348/532
4,933,774	A *	6/1990	Ishimaru	358/335
5,157,510	A	10/1992	Quan	
5,305,109	A *	4/1994	Harford	348/737
5,402,488	A *	3/1995	Karlock	380/5
5,410,364	A *	4/1995	Karlock	348/683
5,661,801	A *	8/1997	Sperber	380/204
5,815,630	A *	9/1998	Sato	386/44
5,864,591	A *	1/1999	Holcombe	375/345
5,907,655	A *	5/1999	Oguro	386/94

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO	WO9715142 A1 *	4/1997	H04N/5/782
WO	WO9716022 A1 *	5/1997	H04N/7/167
WO	WO0013413 A1 *	3/2000	H04N/5/913

OTHER PUBLICATIONS

Takiff, Johnathan, Macrovision Hopes it has out-pirated video-tape pirates, 1988, Chicago Tribune, p. 83.*

Qiao et al, Watermarking Methods for MPEG Encoded Video: Towards Resolving Rightful Ownership, 1998, IEEE, pp. 276–285.*

Barr, David, Copy Protection for High-Definition Baseband Video, 2000, IEEE, pp. 174–177.*

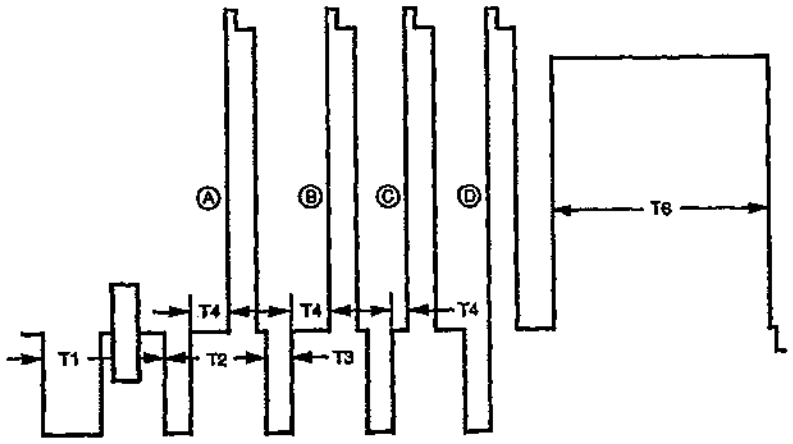
Brendan et al, Technical Challenges of Protecting Digital Entertainment Content, 2003, IEEE, pp. 72–78.*

Primary Examiner—Ayaz Sheikh
Assistant Examiner—Aravind Moorthy
(74) *Attorney, Agent, or Firm*—George Almeida

(57) **ABSTRACT**

A method and apparatus for defeating copy protection signals in a video signal, and also for providing copy protection signals for a video signal, is disclosed. The defeat technique generally utilizes a particular pulse position shifting, modulation, etc., of AGC, normal sync and/or pseudo sync pulses to increase the separation between the pulses. Various embodiments are disclosed including selective shifting of the relative positions of either the sync/pseudo sync or AGC pulses, trimming portions of the sync/pseudo sync and/or the AGC pulses and narrowing of either the sync/pseudo sync and/or the AGC pulses, all to provide the selective position separation between the sync/pseudo sync and AGC pulses. The copy protection technique includes various embodiments for dynamically varying the sync/pseudo sync and AGC pulse separation by applying a modulation of the above position shifting, trimming and/or narrowing techniques over selected time periods to cycle from the copy protection condition to the copy protection defeat condition, back to the copy protection condition.

55 Claims, 13 Drawing Sheets



U.S. PATENT DOCUMENTS

5,953,417 A	*	9/1999	Quan	380/203
6,041,158 A	*	3/2000	Sato	386/1
6,058,191 A	*	5/2000	Quan	380/203
6,173,109 B1	*	1/2001	Quan	386/1
6,188,832 B1	*	2/2001	Ryan	386/94
6,191,725 B1	*	2/2001	Lavoie	342/92
6,295,360 B1	*	9/2001	Ryan et al.	380/54
6,404,889 B1	*	6/2002	Ryan et al.	380/201
6,459,795 B1	*	10/2002	Quan	380/221

* cited by examiner

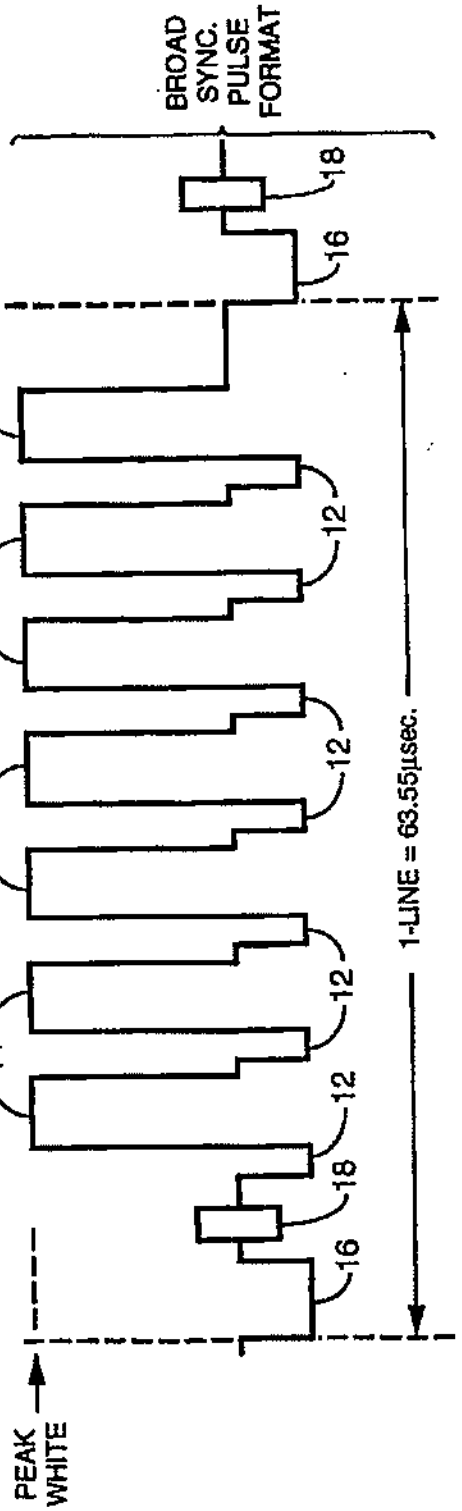


FIG. 1a (PRIOR ART)

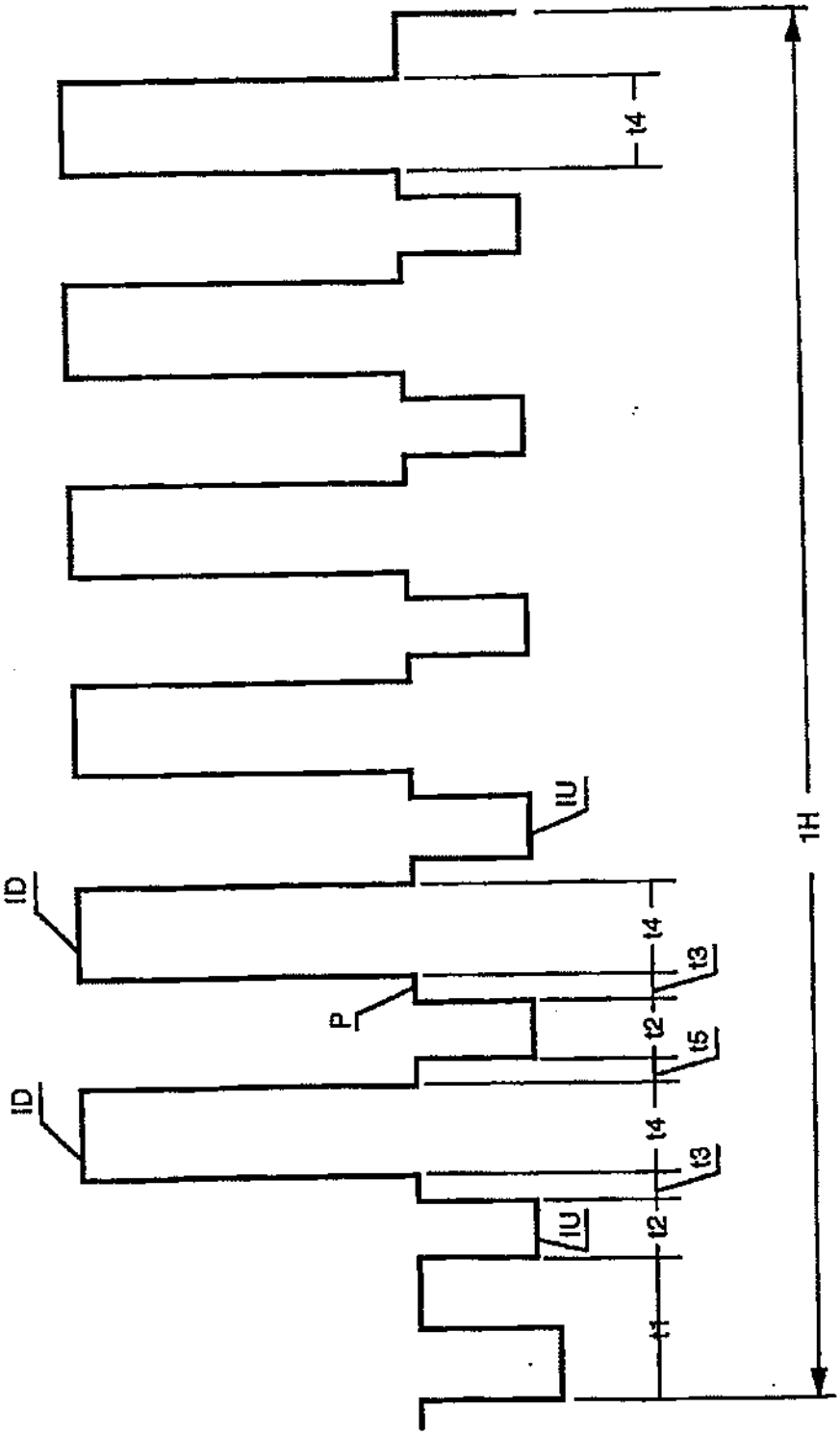


FIG. 1b (PRIOR ART)

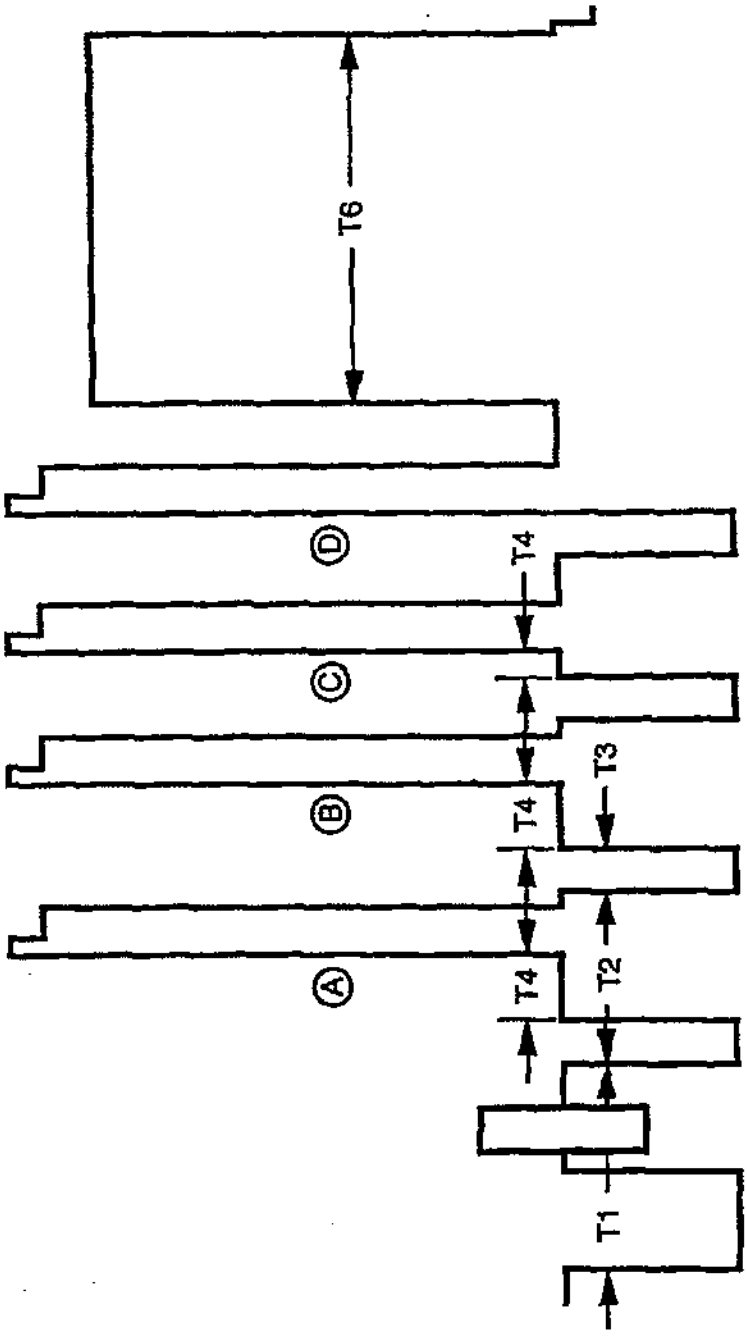


FIG. 2

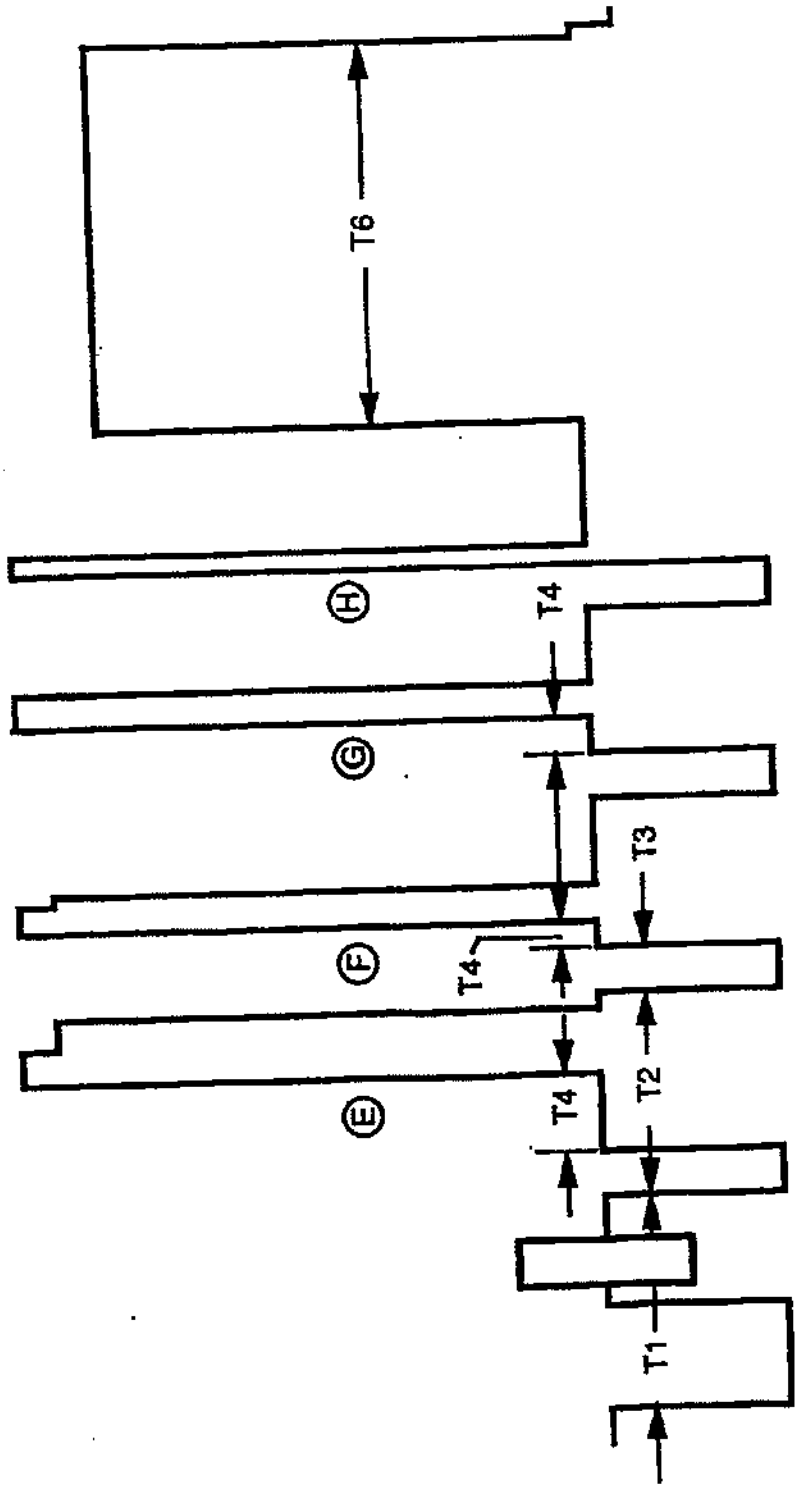


FIG. 3

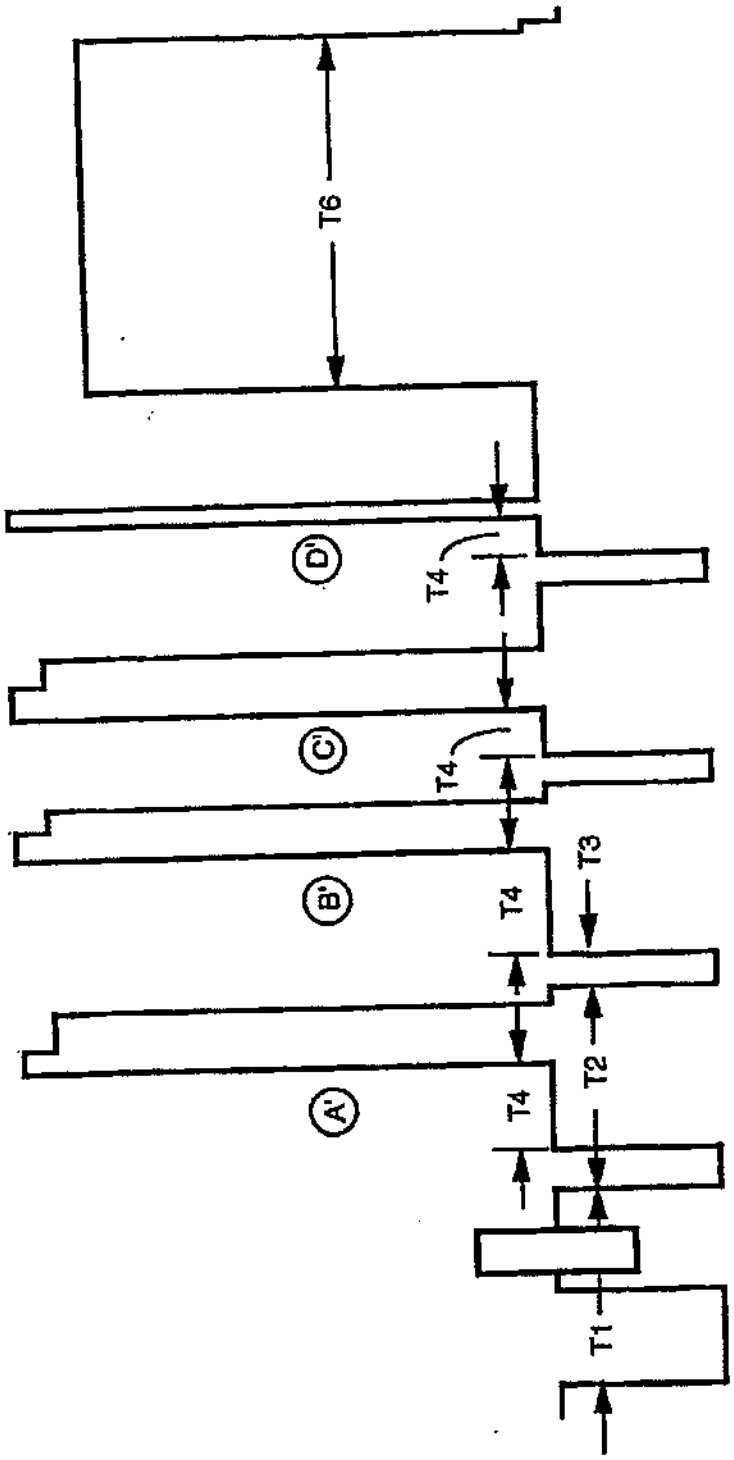


FIG. 4

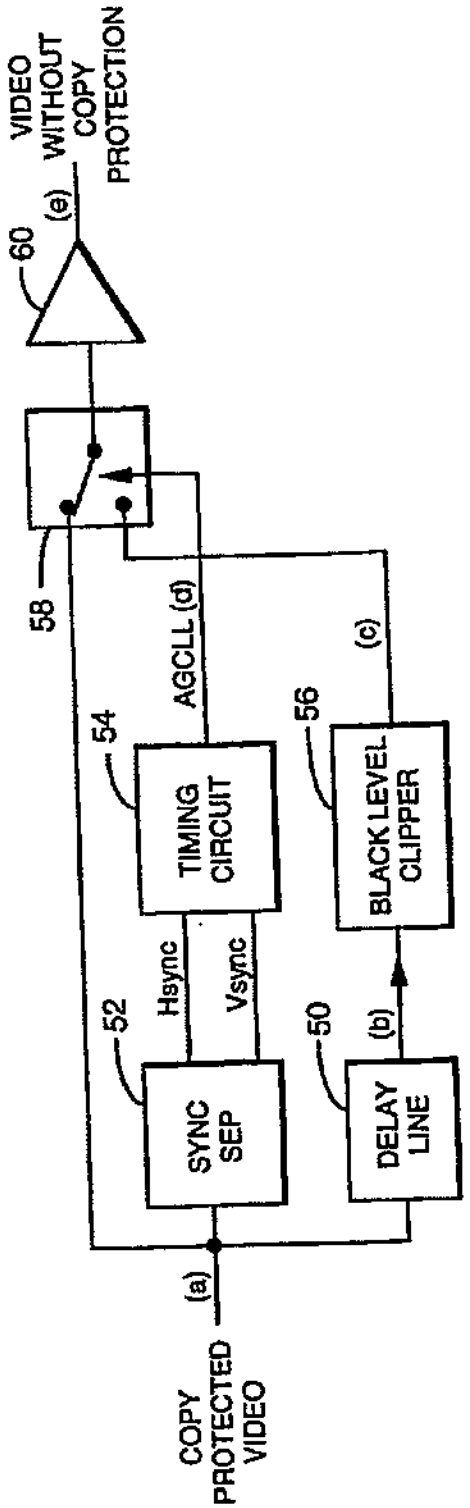

VIDEO WITHOUT COPY PROTECTION
(e)
60
58
AGCLL (d)
(c)
54
56
TIMING CIRCUIT
BLACK LEVEL CLIPPER
Hsync
Vsync
52
50
(b)
SYNC SEP
DELAY LINE
(a)
COPY PROTECTED VIDEO

FIG. 5

FIG. 5a

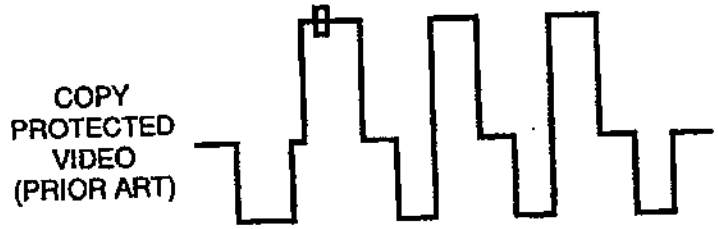


FIG. 5b

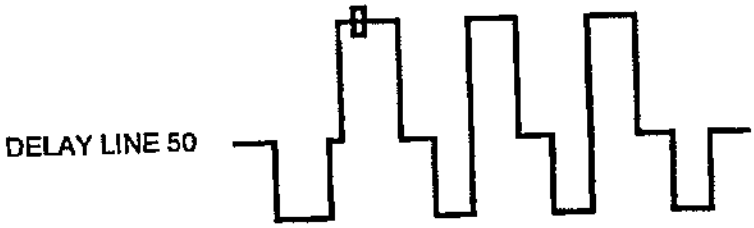


FIG. 5c

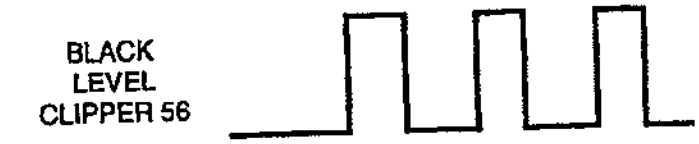
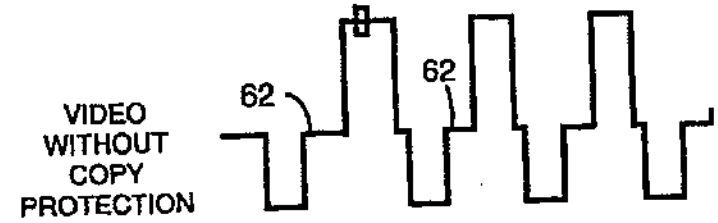


FIG. 5d

FIG. 5e



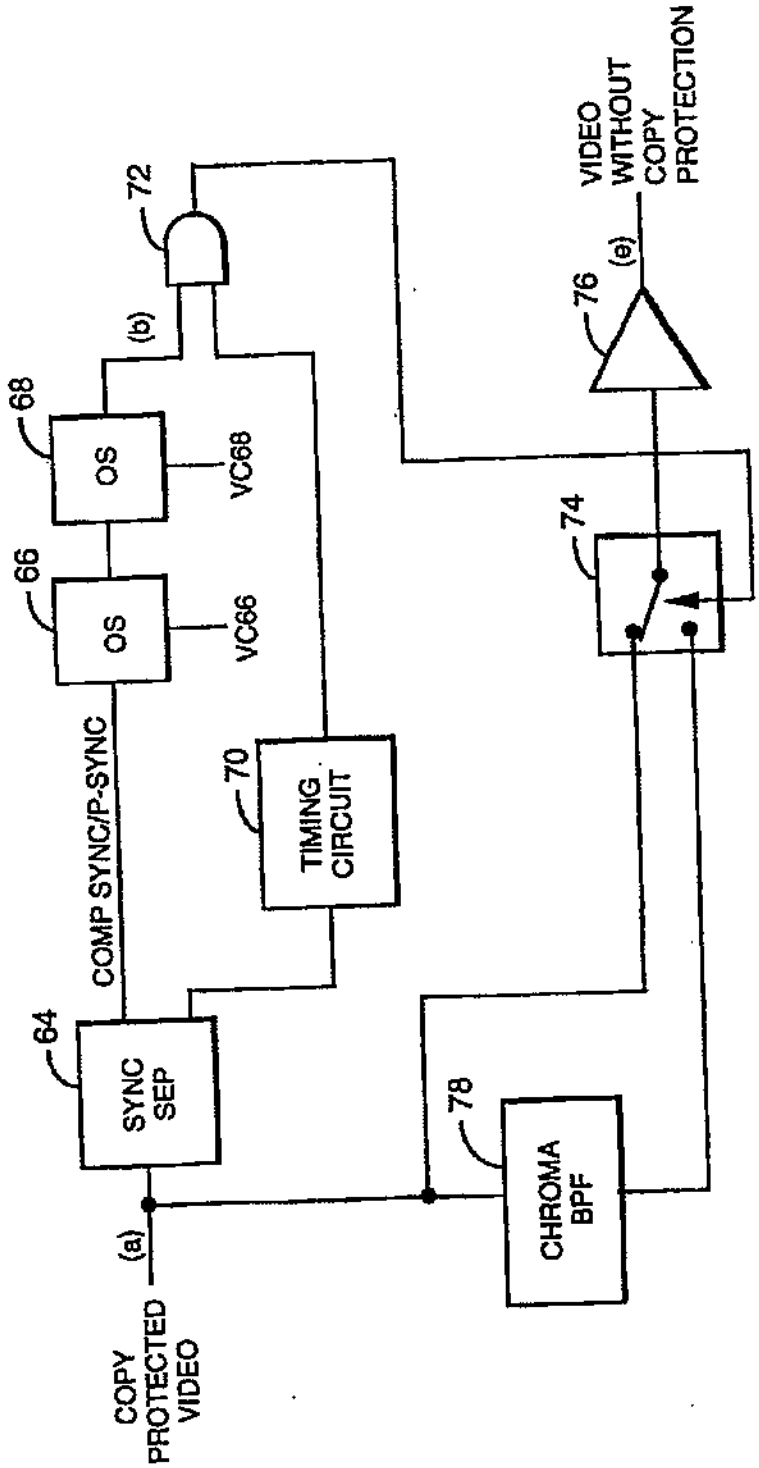

VIDEO WITHOUT COPY PROTECTION
(e)
76
72
(b)
68
OS
VC68
66
OS
VC66
74
COMP SYNC/P-SYNC
70
TIMING CIRCUIT
64
SYNC SEP
78
CHROMA BPF
(a)
COPY PROTECTED VIDEO

FIG. 6

FIG. 6a
(PRIOR ART)

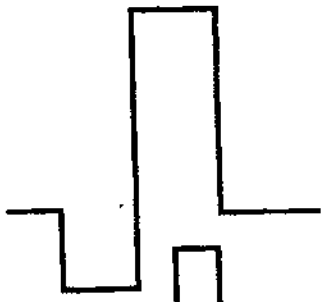


FIG. 6b

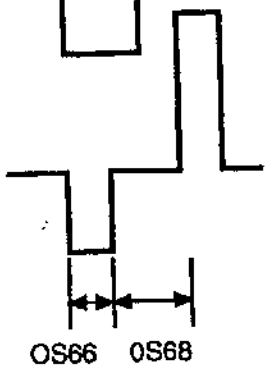


FIG. 6c
(PRIOR ART)

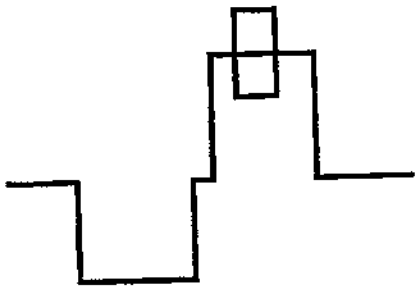


FIG. 6d

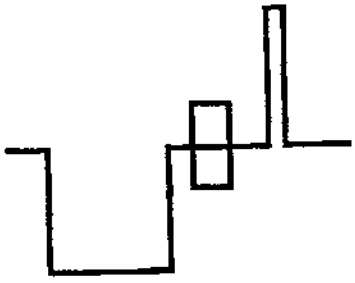
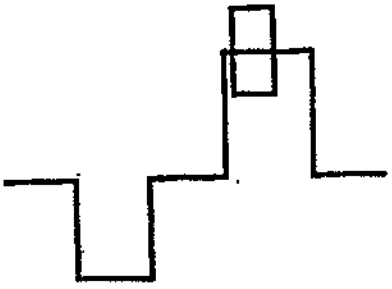


FIG. 6e



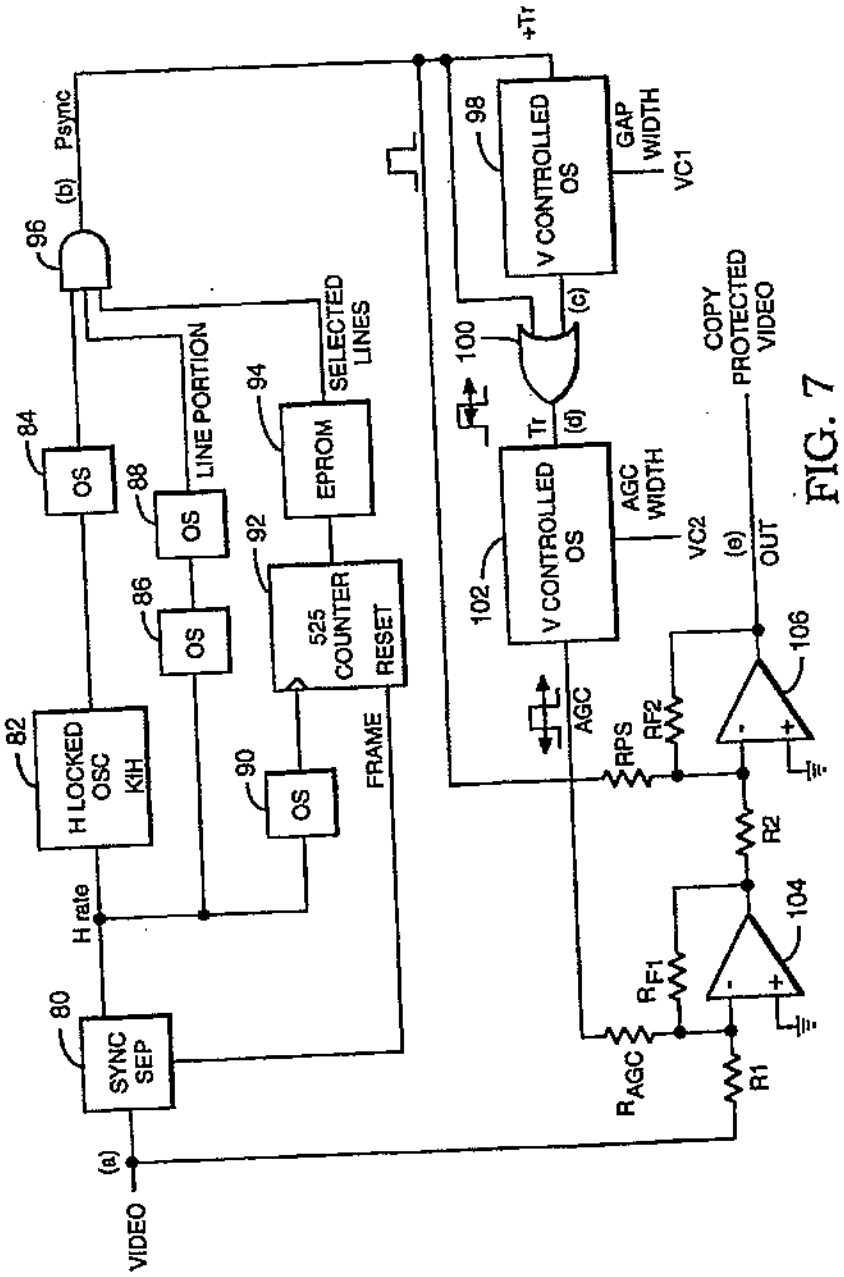

+Tr
Psync
(b)
96
98
V CONTROLLED OS
GAP WIDTH
VC1
SELECTED LINES
94
EPROM
100
(c)
COPY PROTECTED VIDEO
84
OS
88
OS
LINE PORTION
Tr
(d)
AGC WIDTH
VC2
(e)
OUT
V CONTROLLED OS
102
86
OS
92
525 COUNTER
RESET
106
AGC
RPS
RF2
82
H LOCKED OSC KIH
90
OS
FRAME
R2
H rate
104
RF1
80
SYNC SEP
RAGC
R1
(a)
VIDEO

FIG. 7

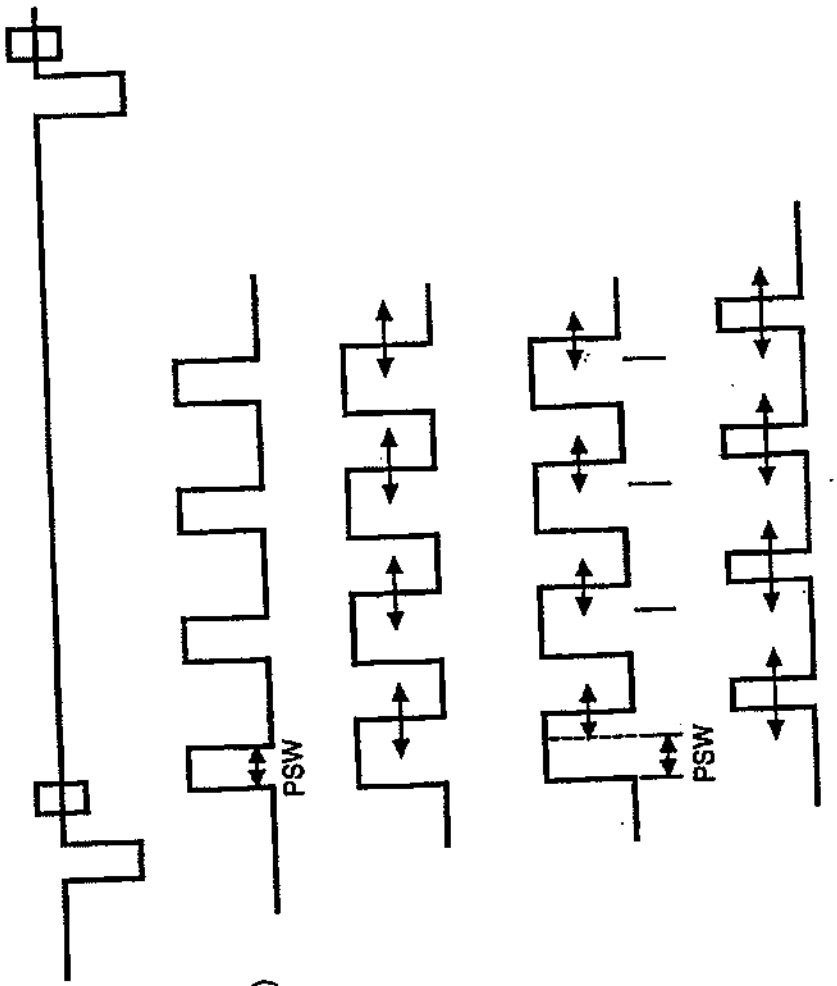


FIG. 7a

FIG. 7b

FIG. 7c

FIG. 7d

FIG. 7e

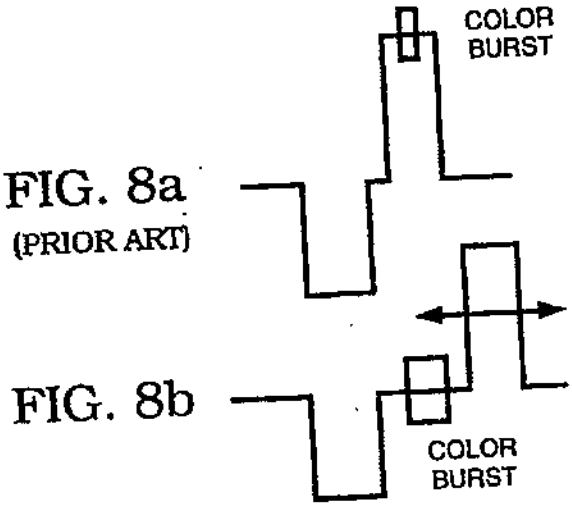


FIG. 8a
(PRIOR ART)

FIG. 8b

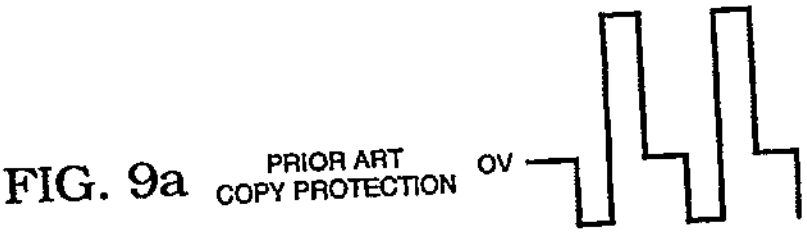


FIG. 9a

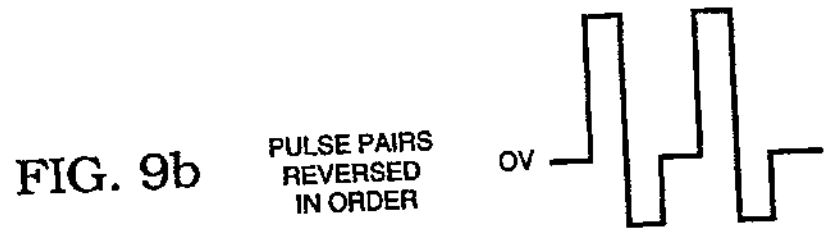


FIG. 9b

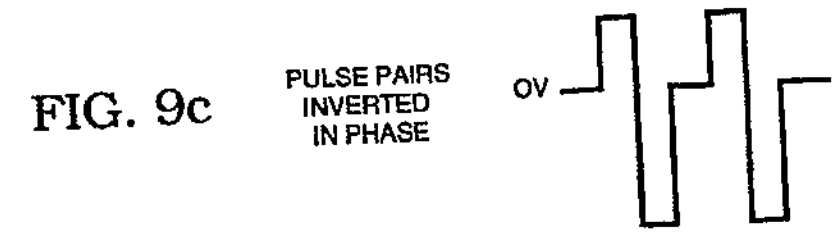


FIG. 9c

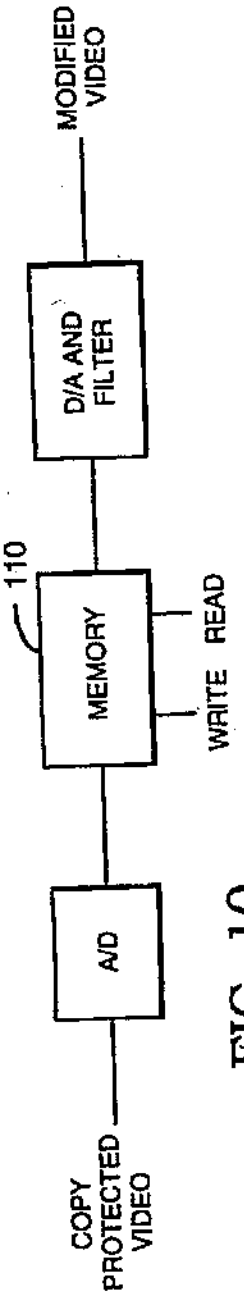

COPY PROTECTED VIDEO
A/D
MEMORY
110
WRITE
READ
D/A AND FILTER
MODIFIED VIDEO

FIG. 10

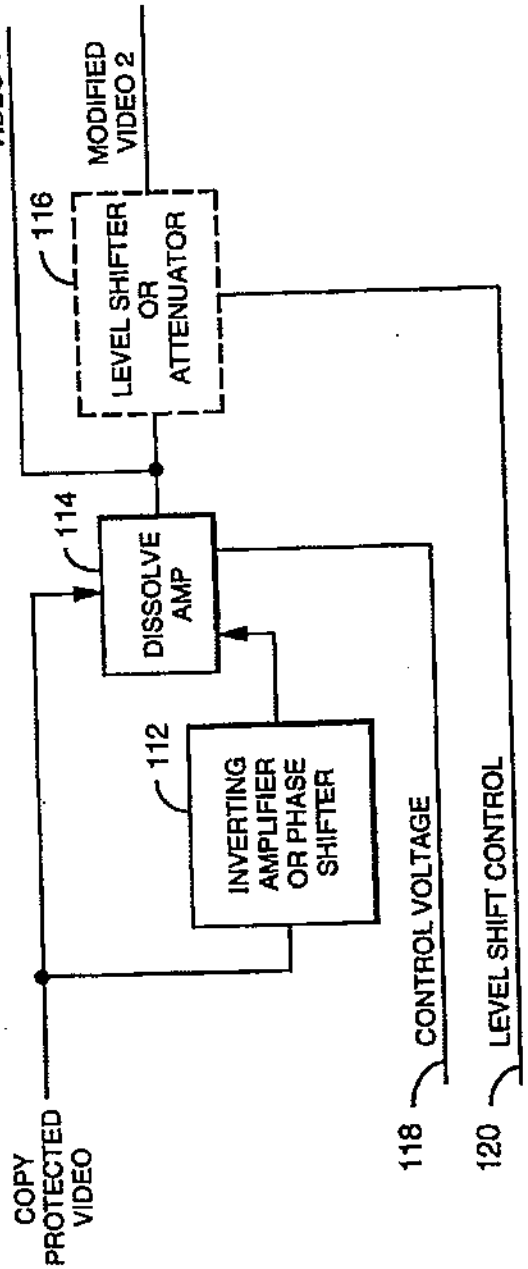

COPY PROTECTED VIDEO
MODIFIED VIDEO 1
MODIFIED VIDEO 2
116
LEVEL SHIFTER OR ATTENUATOR
114
DISSOLVE AMP
112
INVERTING AMPLIFIER OR PHASE SHIFTER
118
CONTROL VOLTAGE
120
LEVEL SHIFT CONTROL

FIG. 11

METHOD AND APPARATUS FOR SYNTHESIZING AND REDUCING THE EFFECTS OF VIDEO COPY PROTECTION SIGNALS

This application claims benefits of Provisional 60/098,804 filed Sep. 2, 1998.

CROSS REFERENCE TO RELATED APPLICATIONS

This invention is related to commonly owned U.S. Pat. No. 4,631,603 entitled "METHOD AND APPARATUS FOR PROCESSING A VIDEO SIGNAL SO AS TO BE ABLE TO PROHIBIT THE MAKING OF ACCEPTABLE VIDEO TAPE RECORDINGS THEREOF" which issued on Dec. 12, 1986; to U.S. Pat. No. 4,695,901 entitled "METHOD AND APPARATUS FOR REMOVING PSEUDO-SYNC PULSES AND/OR AGC PULSES FROM A VIDEO SIGNAL" which issued on Sep. 22, 1987; to U.S. Pat. No. 4,907,093 for METHOD AND APPARATUS FOR PREVENTING THE COPYING OF A VIDEO PROGRAM" which issued Mar. 6, 1990; to U.S. Pat. No. 4,819,098 for "METHOD AND APPARATUS FOR CLUSTERING MODIFICATIONS MADE TO A VIDEO SIGNAL TO INHIBIT THE MAKING OF ACCEPTABLE VIDEO TAPE RECORDINGS" which issued on Apr. 4, 1989; to U.S. Pat. No. 5,157,510 for "METHOD AND APPARATUS FOR DISABLING ANTICOPY PROTECTION SYSTEM IN VIDEO SIGNALS USING PULSE NARROWING which issued on Oct. 20, 1992; to U.S. Pat. No. 5,194,965 for "METHOD AND APPARATUS FOR DISABLING ANTI-COPY PROTECTION SYSTEM IN VIDEO SIGNALS" issued on Mar. 16, 1993; to U.S. Pat. No. 5,625,691 for "METHOD AND APPARATUS TO DEFEAT CERTAIN COPY PROTECTION PULSES WITHIN A VIDEO SIGNAL" issued on Apr. 29, 1997; to U.S. Pat. No. 5,633,927 for VIDEO COPY PROTECTION PROCESS ENHANCEMENT TO INTRODUCE HORIZONTAL AND VERTICAL PICTURE DISTORTIONS" issued on May 27, 1997; to U.S. Pat. No. 5,748,733 for "METHOD AND APPARATUS TO REDUCE EFFECTS OF CERTAIN COPY PROTECTION PULSES WITHIN A VIDEO SIGNAL" issued on May 5, 1998; to U.S. Pat. No. 5,661,801 for "METHOD AND APPARATUS FOR STABILIZING AND BRIGHTENING PRERECORDED TV SIGNALS ENCODED WITH COPY PROTECTION" issued on Aug. 26, 1997; to U.S. Pat. No. 4,336,554 for "CODE SIGNAL BLANKING APPARATUS" issued on Jun. 22, 1982 and to U.S. Pat. No. 5,583,936 for "VIDEO COPY PROTECTION PROCESS ENHANCEMENT TO INTRODUCE HORIZONTAL AND VERTICAL PICTURE DISTORTIONS" issued on Dec. 10, 1996. All of the above are incorporated by reference.

Also related is U.S. Pat. No. 4,163,253 for "METHOD APPARATUS FOR MODIFYING A VIDEO SIGNAL TO PREVENT UNAUTHORIZED RECORDING AND REPRODUCTION THEREOF" issued on Jul. 31, 1979.

BACKGROUND OF INVENTION

1. Field of the Invention

The field of the invention is in the mechanisms and/or methods for defeating, removing, or reducing the effects of the video copy protection signals. These mechanisms are also used to synthesize and improve the performance of a video copy protection signal.

2. Description of the Prior Art

The Hollywood movie industry is very concerned about the unauthorized copying of movies and programs. As an example, on Sep. 17, 1997 Jack Valenti, President and Chief Executive Office of the Motion Picture Association of America stated "If you can't protect what you own—You don't own anything." The patent by Ryan, U.S. Pat. No. 4,631,603, incorporated by reference, discloses a way to process an ordinary program video source to have copy protection. The copy protected video is viewable on a TV set but it produces a recording lacking any entertainment value. That is, the video programs that are not recordable suffer from artifacts ranging from low contrast to synchronizing problems. The '603 patent describes a method for "confusing" or causing misoperation of the AGC system in a videocassette recorder while not causing a black depression problem in a television receiver displaying the copy protected signal.

A Polish Patent Application (PL 304477 ('477)) by Tomasz Urbaniec entitled "Method and Device for Protecting Videophonic Recordings Against Authorized Copying" filed Jul. 28, 1994, hereby incorporated by reference, discloses a variation of the '603 patent by Ryan. FIG. 1*a* of the '603 patent describes the waveform of the copy protected video signal as disclosed by Ryan and is replicated herein as FIG. 1*a*. FIG. 4 of the Urbaniec patent '477 describes the comparative waveform as disclosed by Urbaniec, which is replicated herein as FIG. 1(*b*).

As is well known in the art, the videocassette system has a limited luminance frequency response, less than 2 MHz. A signal as described by Ryan recorded on a videocassette duplicating recorder with the AGC turned off (to avoid the effects of copy protection) will produce a video signal with pulse shapes modified by the limited frequency response of the duplicating recorder. Since there is no gap between the pseudo sync pulses and the AGC pulses of Ryan, the AGC system of a home duplicating recorder will respond to the combination of the pseudo sync pulses and the AGC pulses.

The limited bandwidth of the recording VCR responds slightly differently to the combination of pseudo-sync and AGC pulses separated by a time gap of 0.5 μseconds to 2.0 μseconds. If the time gap is as low as 0.5 μseconds, the limited bandwidth of the recording videocassette recorder distorts the time gap to effectively remove it and the effectiveness of the copy protection is essentially the same as that achieved by Ryan. As the gap widens, the effectiveness of the copy protection is reduced or removed.

To defeat the copy protection process, there are a number of known ways such as attenuating, blanking, narrowing, level shifting, modifying and/or clipping the copy protection pulses as described in U.S. Pat. Nos. 4,695,901 ('901), 4,336,554 ('554), 5,157,510 ('510), 5,194,965 ('965), 5,583,936 ('936), 5,633,927 ('927), 5,748,733 ('733) and 5,661,801 ('801) cited above and hereby incorporated by reference.

In the patents mentioned above, the AGC and/or sync or pseudo sync pulses (see U.S. Pat. No. 4,695,901) are changed in amplitude, changed in level relative to normal sync pulses, and/or changed in pulse width, so as to allow a satisfactory recording.

In particular, U.S. Pat. Nos. 5,194,965 and 5,157,510 disclose narrowing of the AGC and/or pseudo sync pulses so that the record VCR does not sense these narrowed added pulses and thus, makes a satisfactory copy.

SUMMARY OF THE INVENTION

To defeat the anti-copy signal, the present invention discloses a method and apparatus utilizing pulse position

and pulse width modulation of the AGC and/or sync or pseudo sync pulses. The invention also discloses the insertion of a sufficiently wide time gap between the AGC and/or pseudo sync pulses such that the record VCR will respond to or sense the sync or pseudo sync pulses but still will allow for a recordable copy.

The copy protection defeating mechanisms of this invention can also be used in combination with any of the defeat inventions mentioned above. For example, to defeat the copy protection process, one can shift (delay) the AGC pulse by about 1.5 μseconds away from the preceding pseudo sync pulse and then trim the trailing edge of the preceding pseudo sync pulse by 0.6 μsecond. Thus a gap of about 2.1 μseconds exists between the trailing edge of the trimmed pseudo sync pulse and the leading edge of the delayed AGC pulse. If this gap is, for example, near blanking level for 2.1 μseconds, then the VCR will sample the voltage in the gap instead of the added AGC pulses for its AGC amplifier. By sampling this gap voltage near blanking level, the copy protection signal is then nullified. Alternatively, the gap voltage level may be set above or below blanking level. It is important to note that by simply delaying or shifting the position of the leading edge of the AGC pulse relative to the trailing edge of the pseudo sync pulse, the gap between the pseudo sync pulses and the AGC pulses will nullify or partially nullify the effects of the AGC copy protection signal. It is also possible to create this gap in other ways such as moving the trailing edge of pseudo sync pulse away from the leading edge of the upcoming AGC pulse, or some combination of moving the position of both the AGC pulse and pseudo sync pulse to form a gap that would defeat the copy protection process. Typical gap durations of 1.5 μseconds or more have proved effective in defeating the copy protection signal. Compounding the narrowing of the pseudo sync pulses and/or AGC pulses with this gap further enhances defeating the copy protection signal.

It should be noted that the defeat method as described above can be varied and then used as a copy protection signal. By dynamically varying the gap from zero to greater than 1.5 μseconds between the trailing edge of the pseudo sync pulse relative to the leading edge of the upcoming AGC pulse, a new copy protection signal is made to effectively mimic the Ryan '603 patent with amplitude modulated AGC pulses. By varying the gap via position modulation of the pseudo sync pulses relative to the AGC pulse or vice versa, or dynamically narrowing or changing the pulse width of the added pulses (AGC pulse and/or sync or pseudo sync pulse), an easier copy protection implementation is possible in the digital domain and/or analog domain. Today's digital domain is the format of choice for implementing copy protection in cable systems and the like (i.e. digital versatile disc players). The range of pulse widths can be for example, between about 50% to 100% of the normal pulse widths (i.e. the pseudo sync pulse normal widths are about 2.3 μseconds and the AGC normal widths are about 2.3 μseconds to 3 μseconds depending on how many added pulses are in a television (TV) line).

In general the copy protection process of the invention may start having the added pulse pairs as for example in FIG. 2(*a*) of Ryan '603 patent, where the AGC pulse and/or pseudo sync pulse are position separated relative to time. If the gap due to position separation is insufficient to "turn off" the copy protection process (i.e. position modulation amounts to only 1.0 μsecond of gap), then the AGC pulse and/or pseudo sync pulse can be narrowed as a function of time to increase the gap sufficiently (i.e. slowly trim or narrow the AGC pulse and/or pseudo sync pulse by about 0.35 μsecond each, which would add another 0.7 μsecond to the 1.0 μsecond gap for a increased gap duration of 1.7 μseconds). After the gap has been extended as to "defeat" or turn off the copy protection signal, then the new copy protection signal is reactivated by reducing the separation (for example, to zero) between the AGC pulse and pseudo sync pulse and by restoring the pulse widths of the (trimmed or narrowed) AGC pulses and/or pseudo sync pulse to their full normal pulse widths.

The method of using relative position modulation between the sync and AGC pulses for defeating and/or synthesizing a copy protection signal can be applied to the copy protection pulses within or around a horizontal blanking interval. The method can also be combined with narrowing any portion of the added pulses.

In order to produce a further effective copy protection signal, a variation of the U.S. Pat. No. 4,631,603 patent has been developed. To this end, the AGC pulses also are amplitude modulated from full amplitude to zero and vice versa over the period of for example about 20 to 30 seconds. As a result, the illegal copy will have constantly changing brightness levels. This causes more annoyance when compared to a constant dim picture (when the AGC pulses are static and at full amplitude).

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1*a* illustrates a the basic anticopy process consisting of AGC and pseudo sync pulses;

FIG. 1*b* illustrates the Urbaniec modification to the basic anticopy process consisting of AGC and pseudo sync pulses;

FIG. 2 illustrates various ways to position shift the AGC pulse to defeat the copy protection signal. FIG. 2 also shows a way of dynamically shifting the position of the AGC pulse to provide the copy protection process of the invention;

FIG. 3 illustrates a combination of position shifting and narrowing (trimming) the AGC pulses to defeat the copy protection signal. FIG. 3 also shows a way of dynamically shifting the position and then narrowing the AGC pulses in accordance with the copy protection process of the invention;

FIG. 4 illustrates various ways to shift the relative position between AGC pulses and pseudo sync pulses while narrowing pseudo sync and/or AGC pulses to defeat the copy protection signal. If the positional shifting and narrowing of AGC pulses and/or pseudo sync pulses is done from zero to maximum, then this technique can be used as the copy protection signal of the invention;

FIG. 5 illustrates a block diagram of an apparatus for defeating a copy protection signal by delaying the AGC pulses;

FIGS. 5*a* to 5*e* illustrate the waveforms generated at various points in the circuit of FIG. 5;

FIG. 6 illustrates an apparatus for defeating a copy protection process by inserting a time gap between the pseudo sync pulses and the AGC pulses;

FIGS. 6*a* to 6E illustrate several waveforms related or generated by the circuit of FIG. 6 given typical copy protection signals as an input;

FIG. 7 illustrates copy protection apparatus of the invention that generates a dynamically variable time gap (around blanking level) between the trailing edge of pseudo sync pulses and the leading edge of AGC pulses;

FIGS. 7*a* to 7*e* illustrate the relevant waveforms that are generated at various points in the circuit of FIG. 7;

FIGS. 8*a* and 8*b* illustrate position delay or modulation of the raised back porches as mentioned in '098 which can be

used as a defeat process or as a copy protection signal. By varying the gap between the trailing edge of (horizontal) normal sync pulses and their raised back porch AGC pulses, the VCR will respond to these as if the raised back porch AGC pulses are being amplitude modulated up and down, which results in yet another dynamic copy protection process of the invention;

FIG. 9*a* illustrates a prior art copy protection signal. FIG. 9*b* illustrates a defeating or modifying method by reversing at least portions of the pseudo sync and/or AGC pulses. FIG. 9*c* illustrates another method for defeating or modifying the original process (FIG. 9*a* for example) by phase shifting (i.e., inverting) portions of the pseudo syncs and/or AGC pulses;

FIG. 10 is a block diagram illustrating a circuit for reversing at least portions of the pseudo sync and/or AGC pulses by way of a memory circuit; and

FIG. 11 is a block diagram illustrating a circuit for inverting or phase shifting portions of the pseudo syncs and/or AGC pulses by way of an inverting or phase shifting amplifier along with a switching or dissolving amplifier. An optional level shifting and/or attenuating circuit is also shown in FIG. 11.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

As previously discussed, FIGS. 1*a* and 1*b* illustrate prior art copy protection and copy protection defeating signals, respectively.

FIG. 2 illustrates various waveforms corresponding to ways that AGC pulses can be delayed to provide the copy protection defeating technique of the invention. First, the waveform D in FIG. 2 illustrates the AGC pulse and pseudo sync pulse at the normal position previously shown in FIG. 1*a* which causes copy protection. Waveforms A to C show various delays or gaps between the trailing edge of pseudo sync pulse and the leading edge of the respective AGC pulse. Waveforms A and B are effective in turning off the copy protection signal while waveform C causes partial reduction or turn off of the copy protection signal. For effective defeat of the copy protection signal it follows that waveforms A and B are preferable.

For a new copy protection signal that is dynamically varied from on to off, one technique of the invention starts for example, with several seconds of the waveform D of FIG. 2 (copy protection on) then transitions to the waveform C of FIG. 2 (copy protection partially on) and then transitions to the waveform B of the FIG. 2 (copy protection turned off). The gap, or separation T4, in FIG. 2 is preferably continuously or discretely changing from zero to greater than about 1.5 μseconds. Waveform A is used to turn copy protection off.

In FIG. 2 (as well as FIGS. 3, 4) the time interval T1 defines the normal sync to the first pseudo sync pulse period, T2 defines the repetition rate of added pseudo sync pulses, T3 defines the pseudo sync pulses' width and T4 defines the gap duration. T6 designates the width of a white reference pulse which may be included as an option.

FIG. 3 illustrates a variation of the embodiment of FIG. 2 with AGC pulse narrowing, although the pseudo sync pulses can be narrowed as well. In the waveform H of FIG. 3, the pulse resembles a narrowed AGC pulse in the patents '510 and '965 of previous mention. While waveform H of FIG. 3 can be used for defeating copy protection signals, it can again also be used as part of a copy protection signal. The waveform D of FIG. 2 represents a normal copy protection signal which can transition to the waveform H of FIG. 3, a signal with a narrowed AGC pulse, and then transition to waveform F of FIG. 3, a signal with a gap and narrowed AGC pulse. Finally the copy protection signal can be turned off by a transition to the waveform G of FIG. 3, where the gap is larger with a narrowed AGC pulse. Waveform E of FIG. 3 is equivalent to waveform A of FIG. 2 and is used to defeat copy protection.

FIG. 4 illustrates pseudo sync pulse narrowing combined with position delay or modulation of varying pulse widths of the AGC pulses to defeat the copy protection process, or form a dynamic copy protection signal.

The waveform D' of FIG. 4 illustrates a defeat process not illustrated in the patents of previous mention by Quan et al '510 and '965. In waveform D' of FIG. 4 the pseudo sync pulse's trailing edge is advanced to provide a narrowed pseudo sync followed by a delayed AGC pulse leading edge to provide a narrowed AGC pulse. The waveform C' of FIG. 4 illustrates a further gap increase in duration between the AGC pulse by position delaying the AGC pulse using an advanced trailing edge to narrow the pseudo sync pulse. The waveform B' of FIG. 4 illustrates a combination of position separation between the AGC pulse and the pseudo sync pulse with narrowed AGC and pseudo sync pulses. As may be seen, waveform A' is generally the equivalent of waveforms A and E of FIGS. 2 and 3, respectively, and also may be used to defeat the effects of copy protection signals.

Alternatively, by employing narrowed pseudo sync pulses and/or AGC pulses that are varied in width, FIG. 4 provides a dynamic copy protection signal of the invention based on dynamically changing the gap (separation) and the amount of narrowing on pseudo sync pulses and/or AGC pulses. For example, the embodiment may start with a waveform D as illustrated in FIG. 2 to provide the copy protection process, then provide narrowing of the AGC pulses and/or pseudo sync pulses to achieve partial copy protection via the waveform C' in FIG. 4, and then transition to a signal such as waveform B' in FIG. 4 to turn off the copy protection. The embodiment then reverses the cycle from waveforms B', to C' and back to D to restore the copy protection.

FIG. 5 is a block diagram depicting an example of circuitry for defeating the copy protection pulses by delaying the AGC pulses relative to the pseudo sync pulses. To this end, copy protected video is inputted as at (a) to a delay line circuit 50, which delays the input video, and also to a sync separator circuit 52. The output of the sync separator circuit provides horizontal and vertical sync pulses to a timing circuit 54 which in turn outputs pulses at (d) coincident with the video lines containing raised back porch AGC pulses and those with AGC pulses. This output signal, AGCLL, is logic high at least from the leading edge of the AGC pulses of the input video signal to the trailing edge of the AGC pulses which appear at an output (b) of the delay line circuit 50 (delayed input video of about 1.5 μseconds or more). A black clipper circuit 56 coupled to the delay line 50 clips off most or all of the sync pulses. Thus, delayed AGC pulses are supplied at the output (c) of the black clipper circuit. By using an electronic switch 58, with control signal AGCLL to switch in the delayed AGC pulses, the copy protection pulses' effects are then defeated or reduced at the output (e) of an amplifier 60.

FIGS. 5*a* through 5*e* illustrate the waveforms generated at different locations of FIG. 5 and is generally self-explanatory. For example, in FIG. 5*e*, the output has a gap, that is, separation 62, corresponding to gap T4 of FIGS. 2-4, long enough between the sync pulses and AGC pulses to

allow recordable copies of the video signal. It should be noted that FIG. 5 is just an illustration of an apparatus for producing position delay of AGC pulses to defeat the copy protection signal. It is also possible to design a position delay equivalently by removing substantially the original copy protection signal or parts of it and then regenerating modified pseudo sync pulses and/or AGC pulses. For instance, the incoming copy protection pulses may be removed and then the pseudo sync pulses inserted in advance of the original pseudo sync pulse, with AGC pulses inserted in delayed relation to the original AGC pulses. Thus a gap voltage is produced between the pseudo sync pulses and AGC pulses that allows for a recordable copy.

FIG. 6 is a block diagram depicting circuitry for creating a time gap around blanking level by trimming off (advancing) the trailing edge of sync and delaying the leading edge of the AGC pulse of the copy protection signal, leading to a recordable copy. This "trimming" is a different form of narrowing not illustrated in the U.S. Pat. No. 5,194,965. Copy protected video is fed at (a) to a sync separator 64 to output composite sync including pseudo sync pulses to a one shot (multivibrator) 66. One shot 66 triggers off the leading edge of sync pulses including pseudo sync pulses, and its pulse width can be controlled via a control voltage VC66. The output (b) of one shot 66 is coupled to another one shot 68 whose pulse width is controlled by another control voltage, VC68. The output (b) of one shot 68 is then a pulse coincident with the latter portion of the sync or pseudo sync pulse and the beginning portion of the AGC pulse of the copy protected input video signal. A sync separator output also is fed to a timing circuit 70 which generates pulses coincident with the copy protection signal within the video lines. The output of the timing circuit 70 and of the one shot 68 are fed to an AND gate 72 to control a switch 74 during the times copy protection pulses are present. The switch 74 receives the copy protected video at (a) and supplies a signal containing a gap voltage between the sync and AGC pulses of copy protection signals, whereby the video signal at an output (c) of an output amplifier 76 allows for a recordable copy. FIG. 6 also uses a chroma bandpass filter 78 to generate the gap, but also to reinsert color burst during narrowing of the normal sync and/or raised back porch. As a matter of fact narrowing and/or attenuation and/or level shifting of any kind on the raised back porch AGC pulses and/or its sync signal can result in a recordable copy (see raised back porch AGC signal as in FIG. 3 of U.S. Pat. No. 4,819,098 by Ryan).

FIGS. 6*a* to 6*e* show the result of this kind of narrowing. FIG. 6*a* represents a typical copy protection signal consisting of pseudo sync pulses and AGC pulses. FIG. 6*b* shows the narrowed pseudo sync pulses and/or AGC pulses with a gap (voltage) in between. FIG. 6*c* shows a horizontal pulse with a raised back porch AGC pulse in typical fashion of a copy protection signal. FIGS. 6*d* and 6*e* show the result of the apparatus of FIG. 6 which narrows the raised back porch AGC pulse (FIG. 6*d*) and/or the horizontal sync pulse (FIG. 6*e*) to allow a recordable copy. Note in FIG. 6*e* the color burst is still present even after narrowing, in the area where burst is normally located.

FIG. 7 is a block schematic diagram depicting circuitry for generating a copy protection process of the invention that mimics the amplitude modulation of AGC pulses by position modulation. Program video with or without copy protection is the input video signal supplied at input (a) to a sync separator 80, which in turn outputs horizontal rate pulses. These horizontal rate pulses are coupled to a horizontal locked (triggered) oscillator 82. The output of this oscillator is preferably but not necessarily locked to the horizontal frequency at a higher frequency (i.e. 4 cycles per half a video line). A one shot (multivibrator) timer circuit 84 defines the positive pulse duration of the horizontal locked oscillator 82. Meanwhile, the sync separator 80 also outputs the horizontal rate pulses to a one shot 86, whose output is coupled to a one shot 88. The latter supplies a gating pulse for the location of pseudo sync pulses in the video line (i.e. 32 μseconds or first half of the video line). The location of the respective video lines that will contain the copy protection pulses is generated by a circuit consisting of a one shot 90, a (525) line counter 92 and an EPROM circuit 94. From the sync seprator 80, horizontal pulses are supplied to the one shot 90 whose output is coincident with the beginning of the video line. A frame reset pulse is fed to the 525 line counter 92 (i.e. for NTSC) along with the horizontal rate pulses for the counter's clock. The counter's output is used to address the memory circuit of EPROM 94, which is programmed to output logic high pulses coincident with those video lines that will have the copy protection pulses. The output (b) of an AND gate 96 then comprises "inverted" pseudo sync pulses on selected video lines (i.e., in the vertical blanking interval).

One method for generating position modulated AGC pulses is to induce pulse width modulation on an inverted pseudo sync pulse signal and then trigger off the trailing edge of this pulse width modulated inverted pseudo sync pulse signal to generate AGC pulses. To this end, the output of AND gate 96 triggers a voltage controlled one shot timer 98 on the leading edge of an "inverted" pseudo sync pulse signal. The output (c) of one shot timer 98 is a pulse with a minimum width of the output of AND gate 96, and a maximum pulse width of 1.5 μseconds (or more) than its minimum pulse width. For example if the output of AND gate 96 has a pulse width of 2.3 μseconds, then the output of one shot timer 98 has pulse widths that vary according to voltage control VC1 from 2.3 μseconds to at least 2.3 μsecond+1.5 μseconds or at least 3.8 μseconds. The output of one shot timer 98 is OR'd by an OR gate 100 with the output of AND gate 96 to ensure that the output (d) of OR gate 100 has a minimum width of the "inverted" pseudo sync pulse from the AND gate. The output of the OR gate 100 triggers on the trailing edge to output AGC pulses whose widths can be controlled voltage wise via a voltage control VC2 supplied to a voltage controlled one shot timer 102. The output of one shot timer 102 then provides AGC pulses that are varying in delay from the pseudo sync pulses' trailing edge on the order of from zero to at least 1.5 μseconds. The output of one shot timer 102 (AGC pulses) is fed to a summing amplifier 104 along with the input video signal. The output of the inverted pseudo sync pulse from AND gate 96 is negatively summed with the output of amplifier 104 via a (negative) summing amplifier 106. The output (e) of amplifier 106 then has position modulated AGC pulses relative to the pseudo sync pulses and is thus a dynamic copy protection signal.

Note FIG. 7 illustrates that the AGC pulses also can be pulse width modulated if the one shot timer 84 is voltage controlled. FIGS. 7*a* to 7*e* show the wave forms generated at various locations (a)-(e) in the circuit of FIG. 7.

FIGS. 8*a*, 8*b* illustrate that the circuit of FIG. 7 can be applied to copy protection pulses with normal sync and raised back porch AGC pulses such as exemplified by FIG. 7*a*. Thus FIG. 8*b* shows a dynamic position modulated copy protection signal that modifies the technique of FIG. 3 of U.S. Pat. No. 4,819,098. The signal shown in FIG. 8*b* can occur in clusters or in selected video lines.

It should be noted that the copy protection process of the present invention can have position, pulse width and/or gap width modulation, and/or amplitude modulation, done on individual pseudo sync pulses, horizontal sync pulses, AGC pulses or raised back porch AGC pulses, over time from maximum separation (defeated copy protection) to minimum separation (full copy protection). For instance if there are 40 added pulse pairs of normal pseudo sync pulses and AGC pulses, one can in any combination slowly increase the separation between the AGC pulses and pseudo sync pulses in any number of pulse pair(s) at a time or all of them at a time until sufficient pulse pairs of copy protection pulse pairs have maximum separation to turn off copy protection. Additionally, one can in any combination slowly decrease the separation from maximum separation (defeated copy protection) to minimum separation (full copy protection).

As a further example, copy protection signals can be applied throughout the vertical blanking interval and its vicinity, and the copy protection signals can include different amounts of added pulses per video line. In one embodiment for example, a single pseudo sync pulse and/or AGC pulse in a video line can be modulated. As previously mentioned, the AGC or raised back porch AGC pulses also can be amplitude modulated in combination with the above-mentioned processes.

FIG. *9a* depicts a waveform of a prior art copy protection signal. FIG. *9b* depicts a waveform of a defeating or modifying method for the signal of FIG. *9a* which reverses the order of at least portions of the pseudo sync and/or AGC pulses. FIG. *9c* is a waveform of another method to defeat or modify the original process (FIG. *9a* for example) by phase shifting, i.e., inverting, at least portions of the pseudo syncs and/or AGC pulses. In the case of FIG. *9c* the phase shift is a 180 degree reversal of pseudo syncs and AGC pulses. Note that the methods described for FIGS. *9b* and *9c* can be applied to those copy protection pulses around or within the horizontal blanking interval. The methods described for FIGS. *9b* and *9c* can of course be combined with relative attenuation, pulse narrowing, level shifting, and/or position modulation copy protection defeating processes.

Also it is possible to use the techniques described for FIGS. *9b* and *9c* to synthesize a copy protection signal. To dynamically turn on and off the copy protection process for example, the technique starts with a copy protection signal as shown in FIG. *9a* (copy protection effectively on). The technique continues for example, by slowly reversing the order of the pseudo syncs with the AGC pulses until the (modified) copy protection signal substantially becomes FIG. *9b* (copy protection effectively off). Similarly, if the technique starts with FIG. *9a* where the copy protection is fully on, then the copy protection process is slowly turned off by inverting (phase shifting), attenuating, level shifting and/or position modulating the pseudo syncs and/or AGC pulses until the (modified) copy protection signal becomes the signal depicted in FIG. *9c*.

Referring to FIG. **10**, by using a video memory **110** and/or a regenerating signal, the waveform of FIG. *9a* can be transformed to that of FIG. *9b*. In this embodiment, the video memory **110** stores for example, the signal of FIG. *9a* wherein however, the signal is read out of memory in reverse order to achieve the signal of FIG. *9b*. Thus, the block diagram of FIG. **10** is an example of circuitry for implementing the latter signal reversing technique for all or selected portions of the pseudo syncs and/or AGC pulses.

FIG. **11** illustrates circuitry for providing the phase shifting technique of previous mention, which transforms the waveform of FIG. *9a* to that of FIG. *9c*. To this end, an inverting (or phase shifting) amplifier **112** inverts (phase shifts) the signal of FIG. *9a*. A video mix dissolve amplifier **114** (or switcher) is used to transform or transition the waveform from that of FIG. *9a* to that of FIG. *9c*. The dissolve amplifier **114** is responsive to a control voltage **118**. Accordingly, FIG. **11** illustrates circuitry for inverting or phase shifting at least portions of the pseudo syncs and/or AGC pulses by way of the inverting or phase shifting amplifier **112** along with the switching or dissolving amplifier **114**. An optional level shifting and/or attenuating circuit **116** is also illustrated in FIG. **11** in phantom line. The level shifting/attenuating circuit **116** is responsive to a level shift control signal **120**.

Although the invention has been described herein relative to specific embodiments, various additional features and advantages will be apparent from the description and drawings, and thus the scope of the invention is defined by the following claims and their equivalents.

What is claimed is:

1. A method of reducing the effects of copy protection signals in one or more selected video lines of a video signal being supplied to a recorder or television (TV) set, wherein the copy protection signals include sync and/or pseudo sync pulses together with respective automatic gain control (AGC) pulses, with the sync/pseudo pulses having a given small position separation, which can be zero separation, from the respective AGC pulses, comprising:

providing the sync/pseudo sync pulses with the trailing edge thereof having the small position separation from the leading edge of respective AGC pulses, wherein the small position separation maintains the copy protection effect; and

shifting the relative position of either the trailing edge of the sync/pseudo sync pulses or the leading edge of the respective AGC pulses with respect to each other, or shifting the relative positions of the trailing edge of the sync/pseudo sync pulses and the leading edge of the respective AGC pulses, to provide a modified position separation between the trailing edge of the sync/pseudo sync pulses and the leading edge of the respective AGC pulses sufficient to reduce the effects of the copy protection signals.

2. The method of claim **1** including:

delaying the leading edge of the AGC pulses relative to the trailing edge of the respective sync/pseudo sync pulses by a time period commensurate with said modified position separation.

3. The method of claim **2** wherein the delay is in the region of 1.0 to 2.5 microseconds.

4. The method of claim **1** including:

advancing the trailing edge of the sync/pseudo sync pulses relative to the leading edge of the respective AGC pulses by a time period commensurate with said modified position separation.

5. The method of claim **4** wherein the advancement is in the region of 1.0 to 2.5 microseconds.

6. The method of claim **1** including:

delaying the AGC pulses in the region of 0.5 to 1.5 microseconds relative to respective sync/pseudo sync pulses, while advancing the trailing edge of the sync/pseudo sync pulses in the region of 0.5 to 1.5 microseconds relative to the delayed respective AGC pulses to obtain said modified position separation.

7. The method of claim **1** including:

narrowing the durations of the sync/pseudo sync pulses and/or the respective AGC pulses, in combination with

the shifting of the relative positions of the sync/pseudo sync and respective AGC pulses.

8. The method of claim 1 wherein the video level of said modified position separation is at a video level in the region of blanking level.

9. The method of claim 1 including:

delaying the AGC pulse relative to the respective sync/pseudo sync pulse to provide a modified position separation that partially defeats the effects of the copy protection signals; and

narrowing the AGC pulse an amount sufficient to defeat or substantially reduce the effects of the copy protection signals.

10. The method of claim 1 including:

advancing the trailing edge of the sync/pseudo sync pulses to provide a narrowed sync/pseudo sync signal;

delaying the leading edge of the respective AGC pulses to provide a narrowed AGC pulse; and

wherein the resulting modified position separation between the sync/pseudo sync pulses and respective AGC pulses is sufficient to reduce the effects of the copy protection signals.

11. The method of claim 1 including:

delaying the position of the AGC pulse;

advancing the trailing edge of the sync/pseudo sync pulses to narrow the sync/pseudo sync pulse; and

wherein the resulting modified position separation between the sync/pseudo sync pulses and the respective AGC pulses is sufficient to reduce the effects of the copy protection signals.

12. The method of claim 1 including:

removing all or sufficient portions of the copy protection signals of sync/pseudo sync and/or respective AGC pulses;

inserting new sync/pseudo sync pulses in advance of the position of the original sync/pseudo sync pulses that are removed; and/or

inserting new AGC pulses in delayed relation to the position of the original AGC pulses;

thereby providing said modified position separation sufficient to reduce the effects of the copy protection signals.

13. The method of claim 1 including:

providing the small position separation between normal sync pulses and respective AGC pulses; and

position modulating the AGC pulses while maintaining said modified position separation between the normal sync pulses and the respective AGC pulses which reduces the effects of the copy protection signals.

14. The method of claim 1 wherein the step of shifting includes:

reversing the order of at least portions of the sync/pseudo sync pulses and respective AGC pulses while maintaining said modified position separation.

15. The method of claim 1 wherein the step of shifting includes:

phase shifting at least portions of the sync/pseudo sync pulses and the respective AGC pulses 180 degrees.

16. The method of claim 1 wherein the modified position separation caused by the shifted positions of the sync/pseudo sync pulses relative to the respective AGC pulses provides the reduction in the effects of the copy protection signals in the recorder or TV set which may include allowing a recording of a viewable copy of the video signal.

17. The method of claim 1 wherein the AGC pulses are raised back porch AGC pulses which are position modulated.

18. Apparatus for reducing the effects of copy protection signal in one or more selected video lines of a video signal being supplied to a recorder or television (TV) set, wherein the copy protection signals include sync and/or pseudo sync pulses together with respective automatic gain control (AGC) pulses, with the sync/pseudo sync pulses having a given small position separation, which can be zero separation, from the respective AGC pulses, comprising:

an input supplying the copy protected video signal with the trailing edge of the sync or pseudo sync pulses and the leading edge of the respective AGC pulses having the given small position separation which maintains the copy protection effect;

timing circuitry responsive to the input and providing timing signals coincident with one or more portions of the copy protection signals and indicative of one or more video lines containing sync/pseudo sync and respective AGC pulses; and

a modifying circuit responsive to the timing circuitry and shifting a position of the sync/pseudo sync pulses or of the respective AGC pulses on said line so as to provide a modified position separation between the trailing edge of the sync or pseudo sync pulses and the leading edge of respective AGC pulses which is of sufficient position separation to reduce or defeat the effects of the copy protection signals.

19. The apparatus of claim 18 wherein:

the timing circuitry includes a sync separating circuit and provides selected sync signals; and

a timing circuit responsive to the sync separating circuit and which provides the timing signals;

wherein the modifying circuit includes a delay circuit which delays one or more portion of the copy protected video signal; and

wherein the apparatus further includes a switching circuit which inserts the delayed AGC pulses into the copy protected video signal in response to the timing signals.

20. The apparatus of claim 18 wherein:

the timing circuit includes a sync separating circuit which provide selected sync signals; and

a timing circuit responsive to the sync separating circuit to provide the timing signals;

wherein the modifying circuit includes a logic circuit responsive to the timing circuit to provide a control signal indicative of the presence of the copy protection signals and of said modified position separation; and

a switching circuit receiving the copy protected video signal for inserting the pulses having the modified position separation into the copy protected video signal in response to the control signal, to modify the widths of the sync/pseudo pulses and/or the respective AGC pulse.

21. The apparatus of claim 18 further comprising:

a chroma filter receiving the copy protected video signal and which inserts colon burst into the video signal.

22. The apparatus of claim 18 wherein the modified position separation provided by the modifying circuit causes the reduction in the effects of the copy protection signals in the recorder or TV set which may include allowing a recording of a viewable copy of the video signal.

23. Apparatus for reducing the effects of copy protection signals of a video signal being supplied to a recorder or

television set, wherein the copy protection signals include sync/pseudo sync and respective automatic gain control (AGC) pulse pairs comprising:

an input supplying the copy protected video signal with the sync/pseudo sync pulses and the respective AGC pulses;

timing circuitry responsive to the input and providing timing signals coincident with one or more portions of the copy protection signals; and

a modifying circuit for modifying the copy protected video signal, wherein the one or more portion of the modified copy protection signal is altered in reverse order in response to the timing signals to provide altered pulse pairs which defeat or reduce the effect of the copy protection signals.

24. The apparatus of claim 23 wherein the copy protected video signal reversing process is implemented for all or selected portions of all or a selected plurality of the sync/pseudo sync pulses and/or respective AGC pulses.

25. Apparatus for reducing the effects of copy protection signals of a video signal being supplied to a recorder or television set, wherein the copy protection signals include sync/pseudo sync and respective automatic gain control (AGC) pulse pairs, comprising:

an input supplying the copy protected video signal having the sync/pseudo sync pulses and the respective AGC pulses which maintain the copy protection effect;

timing circuitry responsive to the input and providing timing signals coincident with one or more portion of the copy protection signals;

a modifying circuit including an inverting amplifier/phase shifter circuit receiving the copy protected video signal and responsive thereto to provide inverted/phase shifted sync/pseudo sync pulses and respective AGC pulses to modify one or more portion of the original sync/pseudo sync and respective AGC pulses.

26. The apparatus of claim 25 including:

a second source of a second control voltage;

level shifter/attenuator means receiving the output of the modifying circuit and responsive to the second control voltage for level shifting/attenuating the inverted/phase shifted sync/pseudo sync pulses and respective AGC pulses.

27. A method of synthesizing copy protection signals in a video signal, employing sync and/or pseudo sync pulses followed by respective automatic gain control (AGC) pulses, comprising:

providing the sync or pseudo sync pulses with the tailing edges thereof generally coincident with the leading edges of respective AGC pulses thereby having essentially small to zero position separation consistent with maintaining copy protection;

dynamically increasing over time the position separation between the sync/pseudo sync pulses and the respective AGC pulses so as to reduce or defeat the effects of the copy protection signals; and

dynamically decreasing over time the position separation between the sync/pseudo sync pulses and the respective AGC pulses to return to the essentially small to zero position separation to maintain copy protection.

28. The method of claim 27 including:

dynamically varying the position separation between at least one sync/pseudo sync pulse and at least one respective AGC pulse from the essentially small to zero position separation to a position separation in the region of 1.5 to 5.0 microseconds.

29. The method of claim 27 including:

dynamically varying the position separation by dynamically varying the advancement of the trailing edge of the sync/pseudo sync pulses with respect to the respective AGC pulses.

30. The method of claim 27 including:

dynamically varying the position separation by dynamically varying the delay of the leading edge of the AGC pulses with respect to the respective sync/pseudo sync pulses.

31. The method of claim 27 including:

dynamically varying the position separation by dynamically varying the advancement of the sync/pseudo sync pulses while dynamically varying the delay of the respective AGC pulses.

32. The method of claim 27 including:

dynamically varying the position separation by dynamically varying the pulse width or the pulse width duration of the AGC pulses and/or of the sync/pseudo sync pulses.

33. The method of claim 27 including:

dynamically narrowing any portion or all of the AGC pulses and/or the sync/pseudo sync pulses.

34. The method of claim 33 wherein the pulse width of the sync/pseudo sync and/or AGC pulses are narrowed in the region of 100 percent to 50 percent.

35. The method of claim 27 wherein only the AGC pulses are shifted in position continuously or discretely.

36. The method of claim 27 further comprising:

dynamically amplitude modulating the sync pseudo sync and/or the AGC pulse.

37. The method of claim 27 further comprising:

narrowing any portion of the sync, pseudo sync and/or AGC pulses.

38. The method of claim 27 wherein the AGC pulses are shifted in position or are narrowed continuously or discretely to dynamically enable and disable the copy protection signals.

39. The method of claim 27 wherein the position separation or gap between the sync or pseudo sync pulse and the respective AGC pulse is gap width modulate.

40. The method of claim 27 wherein:

the dynamic increasing and decreasing of the position separation comprises position and/or pulse width modulating the sync/pseudo sync and/or the AGC pulses; and

amplitude modulating the position and/or pulse width modulated sync/pseudo sync and/or AGC pulses.

41. Apparatus for synthesizing copy protection signals in a video signal employing sync and/or pseudo sync pulses followed by respective automatic gain control (AGC) pulses, comprising:

timing circuitry receiving the video signal and which provides timing signals indicative of video lines which are to contain the copy protection signals, and of the location in the video lines of selected copy protection signals;

a generating circuit to generate selectively derived and modulated pseudo sync pulses, which are modulated in response to the timing circuitry, and which generate AGC pulses that vary in width and/or position in response to the respective selectively derived and modulated pseudo sync pulses; and

a summing/inserting circuit receiving the video signal and responsive to the generating circuit and the timing

circuitry to add or insert to the video signal a dynamic copy protection signal formed of the pseudo sync pulses and the respective width and/or position modulated AGC pulses.

42. The apparatus of claim 41 wherein:

the timing circuitry includes a sync separating circuit to provide a horizontal rate (H rate) signal;

a first circuit responsive to the H rate signal to provide a first signal which defines a positive pulse duration of an H rate related signal;

a timing generator responsive to the H rate signal and which provides a second signal indicative of the location of sync pulses in a video line;

a line circuit responsive to the H rate signal to provide a third signal indicative of the video lines which are to contain the copy protection signals; and

a logic circuit responsive to the first, second and third signals to provide inverted pseudo sync pulses on selected video lines;

wherein the generating circuit includes a timer circuit responsive to control voltages to provide said AGC pulses that are varying in width and in position; and

the summing/inserting circuit includes a summing amplifier receiving the video signal and responsive to said selectively derived pseudo sync pulses and said width and position varying AGC pulses, wherein the summing/inserting circuit provides the position modulated AGC pulses in combination with the derived pseudo sync pulses, resulting in a dynamically varying copy protected video signal.

43. The apparatus of claim 42 wherein:

said first circuit includes an H locked oscillator responsive to the H rate signal;

said line circuit includes a memory responsive to a line counter;

said timer circuit includes a pair of voltage controlled circuits; and

said summing amplifier includes first and second summing amplifiers responsive to said derived pseudo sync pulses and said respective width and position delay varying AGC pulses.

44. The apparatus of claim 41 wherein:

the copy protection signals include sync, pseudo sync, AGC and/or raised bark porch AGC pulses; and

said generating circuit provides dynamic position, pulse width and/or gap width modulation of the pulses.

45. Apparatus for synthesizing copy protection signals in a video signal employing sync and/or pseudo sync pulses followed by respective automatic gain control (AGC) pulses, comprising:

a generating circuit for providing the respective AGC pulses within at least a portion of a back porch; and

wherein said generating circuit dynamically positions and/or width modulates the respective back porch AGC pulses to vary from maintaining to reducing copy protection effects or to vary from reducing to maintaining copy protection effects.

46. A method of providing copy protection signals in a video signal and for reducing the effects or effectiveness of the copy protection signals when desired, wherein the copy protection signals include sync and/or pseudo sync pulses and respective automatic gain control (AGC) pulses, comprising:

providing the sync/pseudo sync pulses with the trailing edges thereof coincident with, or separated by less than 1.0 microsecond from, the leading edges of respective AGC pulses to provide the copy protection signals; and

position separating relative to time the sync/pseudo sync pulses relative to the respective AGC pulses sufficient to provide the reduction in the effects or effectiveness of the copy protection signals.

47. A method of reducing the effects or effectiveness of copy protection signals in one or more selected video lives of a video signal being supplied to a recorder or television (TV) set, wherein the copy protection signals include negative going pulses and respective positive going pulses, with the negative going pulses having a given small position separation, which may be zero separation, from the respective positive going pulses, comprising:

providing the negative going pulses with the trailing edge thereof having the small position separation from the leading edge of respective positive going pulses, wherein the small position separation maintains the copy protection effect; and

shifting the relative position of either the trailing edge of the negative going pulses or the leading edge of the respective positive going pulses with respect to each other, or shifting the relative positions of the trailing edge of the negative going pulses and the leading edge of the respective positive going pulses, to provide a modified position separation between the trailing edge of the negative going pulses and the leading edge of the respective positive going pulses sufficient to reduce the effect of the copy protection signals.

48. Apparatus for reducing the effects or effectiveness of copy protection signals in one or more selected video lines of a video sisal being supplied to a recorder or television (TV) set, wherein the copy protection signals include negative going pulses and respective positive going pulses, with the negative going pulses having a given small position separation, which may be zero separation, from the respective positive going pulses, comprising:

input means supplying the copy protected video signal with the trailing edge of the negative going pulses and the leading edge of the respective positive going pulses having the given small position separation which maintains the copy protection effect;

timing circuitry responsive to the input means and providing timing signals coincident with one or more portions of the copy protection signals and indicative of one or more video lines containing the negative going pulse and the relative positive going pulses; and

circuit means responsive to the timing circuitry and shifting the relative edges and/or positions of the negative going pulses and of the respective positive going pulses with respect to each other so as to provide a modified position separation between the trailing edge of the negative going pulses and the leading edge of the positive going pulses which is of sufficient position separation to reduce or defeat the effects of the copy protection signals.

49. A method of synthesizing copy protection signals in a video signal, employing sync and/or pseudo sync pulses followed by respective automatic gain control (AGC) pulses and/or raised back porch AGC pulses, comprising:

dynamically modulating at least one or a selected combination of a position, gap width, pulse width or amplitude of one or more of selected pulses of the sync, pseudo sync, AGC and/or raised back porch AGC pulses so as to synthesis the copy protection signals.

50. The method of claim 49 further including selected raised back porch pulses, wherein the selected raised back

porch pulses are position modulated or position delayed to assist in said synthesis.

51. The method of claim 49 wherein only the AGC or raised back porch AGC pulses are position and/or pulse width modulated.

52. The method of claim 49 wherein only the sync and/or pseudo sync pulses are position and/or pulse width modulated.

53. A method of synthesizing copy protection signals in a video signal, employing sync, pseudo sync and respective automatic gain control (AGC) pulses, comprising:

dynamically modulating the position, pulse width and/or gap width of the AGC pulses or of the sync/pseudo sync pulses, wherein a single AGC and/or pseudo sync pulse is modulated to vary from maintaining to reducing copy protection effects or to vary from reducing to maintaining copy protection effects.

54. The method of claim 53 wherein the modulating includes amplitude modulation.

55. The method of claim 53 wherein any of a selected number and arrangement of AGC pulses are modulated to enable and disable the copy protection signal.

* * * * *

US006381747B1

(12) **United States Patent**
Wonfor et al.

(10) **Patent No.: US 6,381,747 B1**
(45) **Date of Patent: Apr. 30, 2002**

(54) **METHOD FOR CONTROLLING COPY PROTECTION IN DIGITAL VIDEO NETWORKS**

(75) Inventors: **Peter J. Wonfor**, El Granada; **Derek T. Nelson**, Menlo Park, both of CA (US)

(73) Assignee: **Macrovision Corp.**, Sunnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/142,039**

(22) PCT Filed: **Mar. 31, 1997**

(86) PCT No.: **PCT/US97/05257**

§ 371 Date: **Aug. 31, 1998**

§ 102(e) Date: **Aug. 31, 1998**

(87) PCT Pub. No.: **WO97/37492**

PCT Pub. Date: **Oct. 9, 1997**

Related U.S. Application Data

(60) Provisional application No. 60/014,684, filed on Apr. 1, 1996.

(51) **Int. Cl.**[7] **H04N 7/173**

(52) **U.S. Cl.** **725/104**; 386/94; 380/201; 380/203

(58) **Field of Search** 348/3, 5.5, 7, 10, 348/12; 386/1, 94; 360/60; 380/201, 203, 204; 725/104, 8, 30, 146, 1, 2, 31, 25

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,631,603	A	* 12/1986	Ryan	360/37.1
4,890,319	A	* 12/1989	Seth-Smith et al.	380/5
4,914,694	A	* 4/1990	Leonard et al.	380/5
5,315,448	A	5/1994	Ryan	
5,418,853	A	* 5/1995	Kanota et al.	380/5
5,574,787	A	* 11/1996	Ryan	380/5
5,654,747	A	* 8/1997	Ottesen et al.	348/12
5,675,647	A	* 10/1997	Garneau et al.	380/20
5,680,457	A	* 10/1997	Bestler et al.	380/21
5,737,417	A	* 4/1998	Buynak et al.	380/5
6,002,694	A	* 12/1999	Yoshizawa et al.	370/486
6,002,830	A	* 12/1999	Quan	386/1
RE36,763	E	* 7/2000	Kanota et al.	380/5

FOREIGN PATENT DOCUMENTS

EP	0691787	1/1996

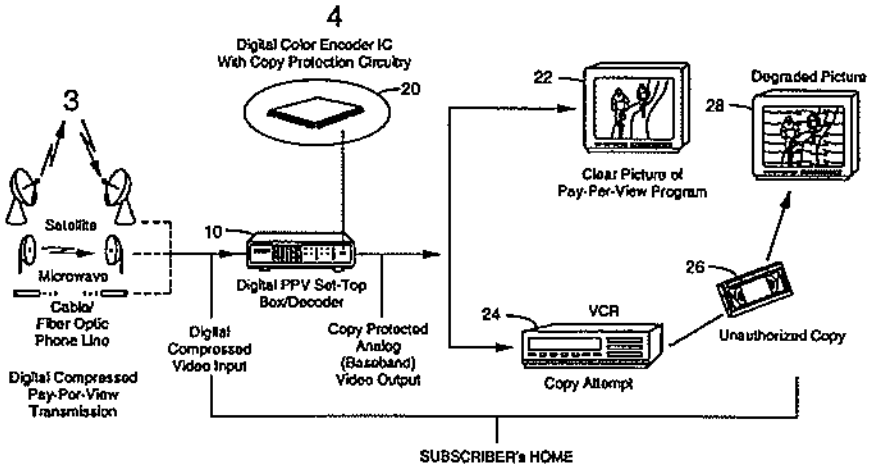
* cited by examiner

Primary Examiner—Andrew Faile
Assistant Examiner—Ngoc Vu
(74) *Attorney, Agent, or Firm*—George Almeida; Frank Nguyen

(57) **ABSTRACT**

A method and system of providing copy protection of video analog and digital signals and the like, wherein the signals are transmitted via a digital delivery network, and may comprise, for example, pay per view (PPV) program materials protected by copyrights of respective program rights holders. The right holders authorize video service providers (3) to apply copy protection to the program material. The copy protection process is supplied to the rights holders or the service providers (3) by a copy protection process licensor. The video service providers (3) supply suitable copy protection control software via respective control and billing (tracking) centers to generate commands which activate, control and reconfigure the copy protection process being applied to the programs being transmitted. A settop box (10) is provided to each consumer and contains a copy protection circuit which is adapted to apply selected anti-copy waveforms to the video signal corresponding to the program material in response to the commands from the service providers (3). Usage data pertinent to each consumer is returned by the settop box (10) to the service providers (3), which then report the copy protection usage to the respective rights holders and process licensor.

52 Claims, 3 Drawing Sheets



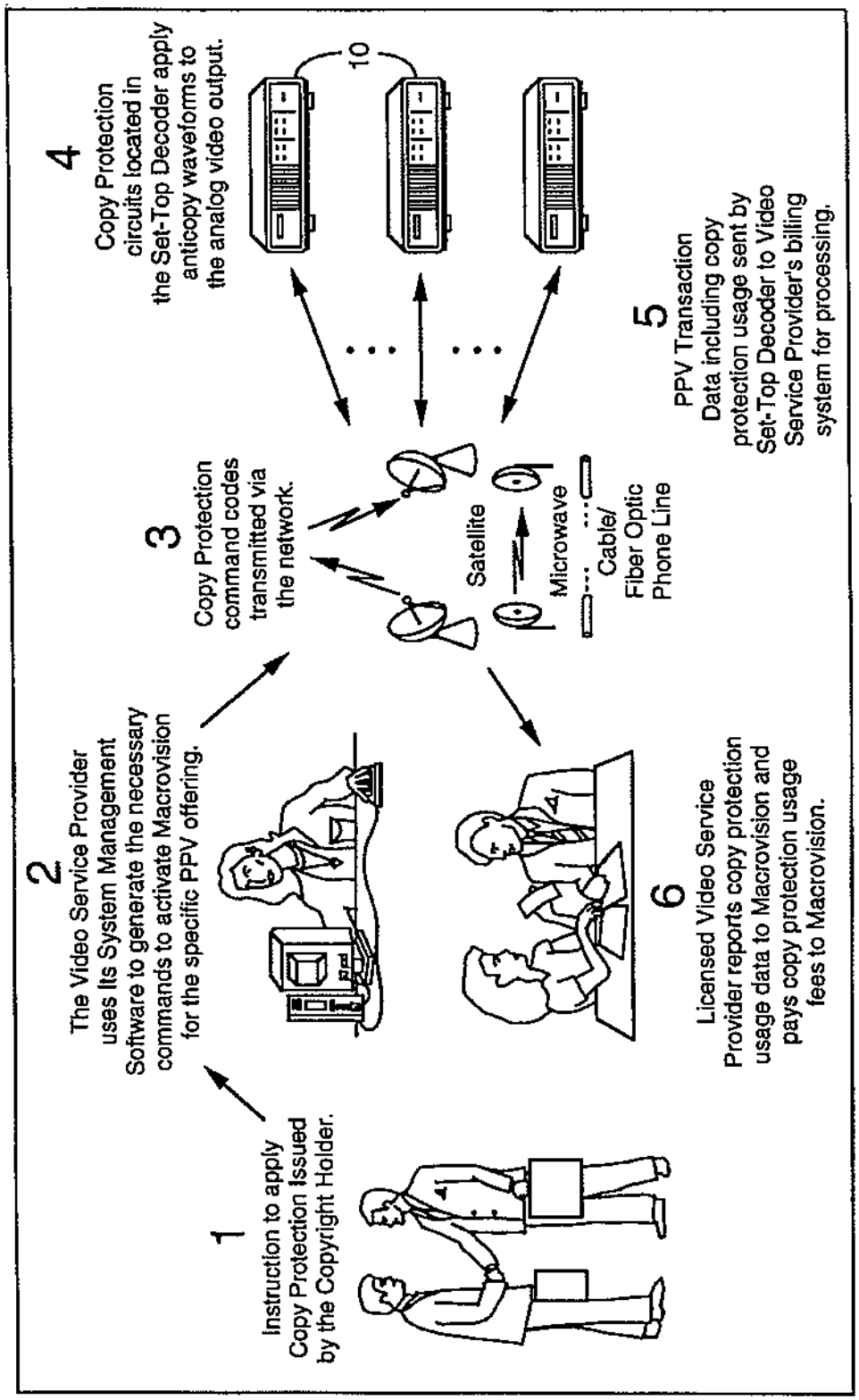

1
Instruction to apply Copy Protection Issued by the Copyright Holder.
2
The Video Service Provider uses Its System Management Software to generate the necessary commands to activate Macrovision for the specific PPV offering.
3
Copy Protection command codes transmitted via the network.
Satellite
Microwave
Cable/ Fiber Optic Phone Line
4
Copy Protection circuits located in the Set-Top Decoder apply anticopy waveforms to the analog video output.
10
5
PPV Transaction Data including copy protection usage sent by Set-Top Decoder to Video Service Provider's billing system for processing.
6
Licensed Video Service Provider reports copy protection usage data to Macrovision and pays copy protection usage fees to Macrovision.

FIG. 1

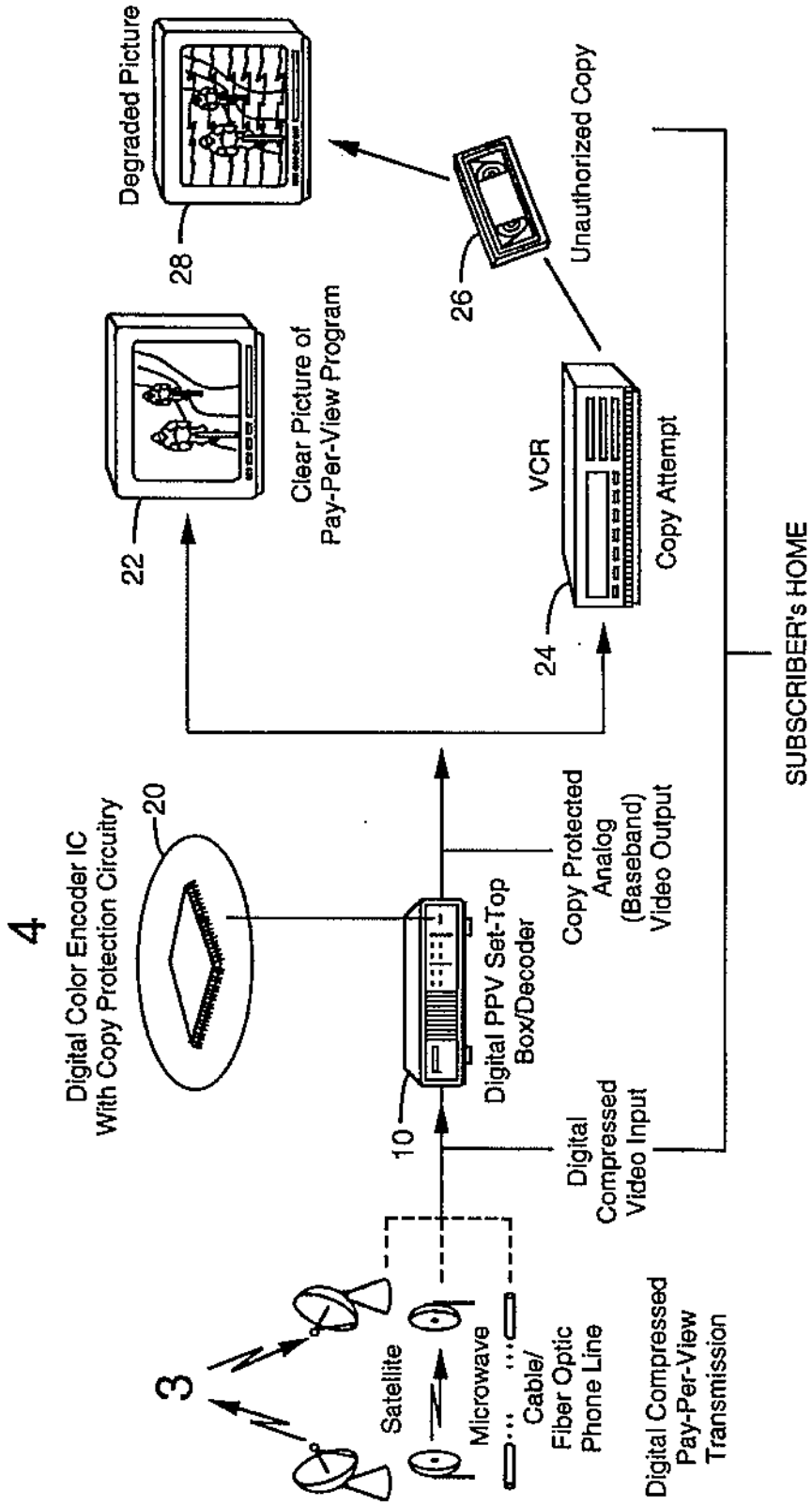

Degraded Picture
28
Unauthorized Copy
26
Clear Picture of Pay-Per-View Program
22
VCR
Copy Attempt
24
SUBSCRIBER's HOME
4
Digital Color Encoder IC With Copy Protection Circuitry
20
Digital PPV Set-Top Box/Decoder
10
Copy Protected Analog (Baseband) Video Output
Digital Compressed Video Input
3
Satellite
Microwave
Cable/ Fiber Optic Phone Line
Digital Compressed Pay-Per-View Transmission

FIG. 2

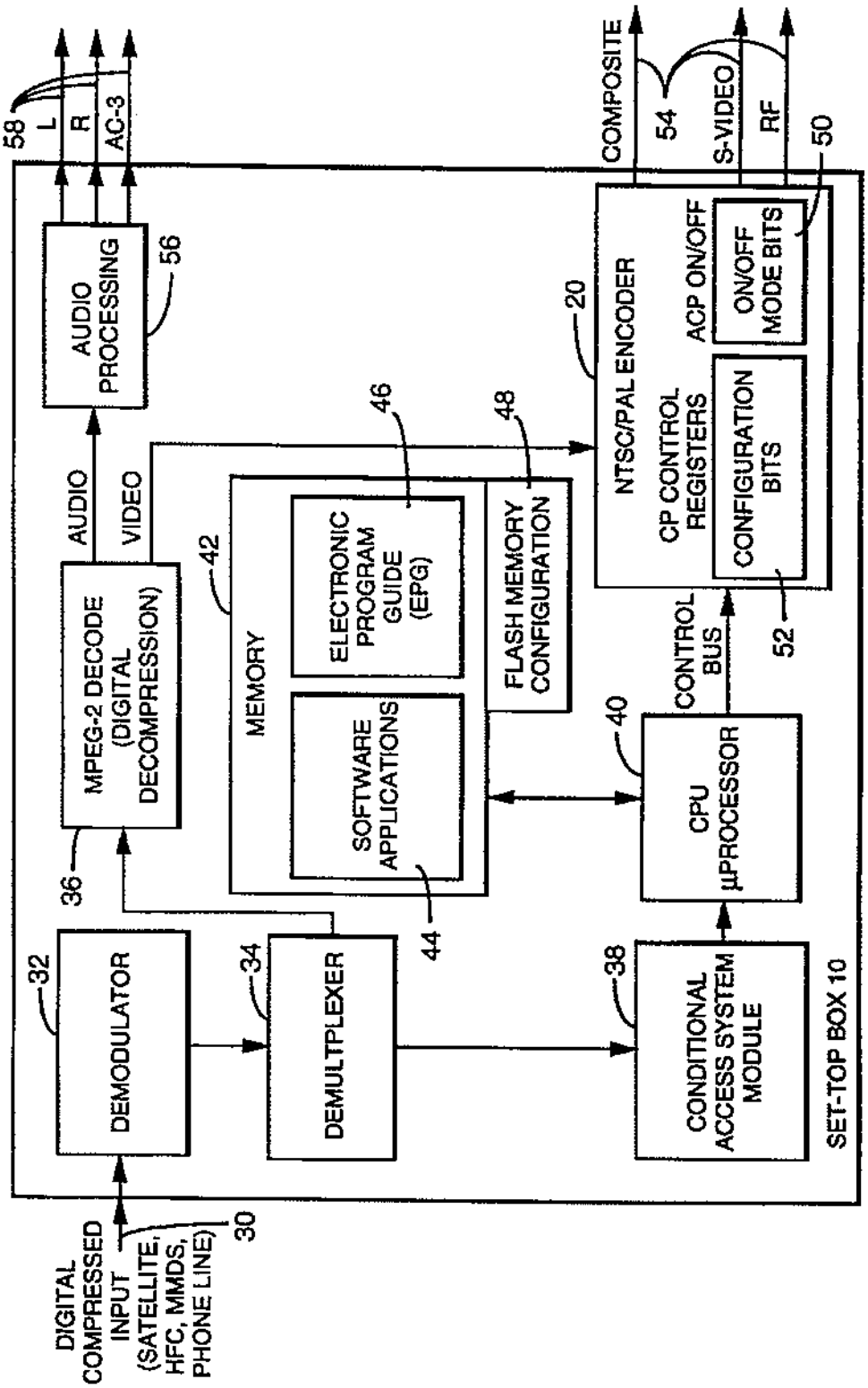

58
L
R
AC-3
COMPOSITE
54
S-VIDEO
RF
50
AUDIO PROCESSING
56
20
NTSC/PAL ENCODER
ACP ON/OFF
ON/OFF MODE BITS
CP CONTROL REGISTERS
CONFIGURATION BITS
46
48
AUDIO
VIDEO
42
MEMORY
ELECTRONIC PROGRAM GUIDE (EPG)
FLASH MEMORY CONFIGURATION
SOFTWARE APPLICATIONS
MPEG-2 DECODE (DIGITAL DECOMPRESSION)
CONTROL BUS
52
40
CPU µPROCESSOR
36
44
32
34
38
DEMODULATOR
DEMULTIPLEXER
CONDITIONAL ACCESS SYSTEM MODULE
SET-TOP BOX 10
DIGITAL COMPRESSED INPUT (SATELLITE, HFC, MMDS, PHONE LINE)
30

FIG. 3

METHOD FOR CONTROLLING COPY PROTECTION IN DIGITAL VIDEO NETWORKS

This application claims the benefit of 60/014,684, filed Apr. 1, 1996.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This disclosure is directed to a method of controlling copy protection in digital video networks where it is desired to copy protect an analog or digital video output signal associated with a digital video network.

2. Background of the Invention

Various well known copy protection schemes for video signals include that disclosed in U.S. Pat. No. 4,631,603, John O. Ryan, Dec. 23, 1986 and assigned to Macrovision Corporation, incorporated by reference, directed to modifying an analog video signal to inhibit making of acceptable video recordings therefrom. This discloses adding a plurality of pulse pairs to the otherwise unused lines of a video signal vertical blanking interval, each pulse pair being a negative-going pulse followed closely by a positive-going pulse. The effect is to confuse AGC (automatic gain control circuitry) of a VCR (video cassette recorder) recording such a signal, so that the recorded signal is unviewable due to the presence of an excessively dark picture when the recorded signal is played back.

Another analog video protection scheme is disclosed in U.S. Pat. No. 4,914,694 issued Apr. 3, 1990, to Leonard, and assigned to Eidak Corp., incorporated by reference. The Eidak system (see Abstract) increases or decreases the length of each video field from the standard length, either by changing the time duration of the respective horizontal line intervals in each field while keeping a constant, standard number of lines per frame, or by changing the number of horizontal line intervals which constitute a frame while maintaining the standard duration of each line interval.

These video protection systems modify the video signal to be recorded (for instance on tape) or to be broadcast (for instance protected pay-per-view television programs) to make copying by ordinary VCRs difficult or impossible. When a video tape on which is recorded the copy protected video signal is played back for viewing using a VCR, the copy protection process is essentially transparent, i.e., it does not interfere with viewing. However, any attempt made to copy the video signal from the tape using a second VCR to record the output of the first (playback) VCR yields a picture degraded to some extent, depending on the efficacy of the particular copy protection system. These present video copy protection systems protect only analog video signals, which are the type of video signals broadcast and recorded using current consumer video technology.

Some digital and hybrid solutions to the copy protection problem were solved by U.S. Pat. No. 5,315,448, issued May 24, 1994, issued to Ryan and assigned to Macrovision Corporation, incorporated by reference. This patent is directed to copy protection for use with digital signal recording where it is desired to copy protect both an analog and digital signal associated with a digital VCR, and any signal material where the original source material is not copy protectable.

A fundamental revolution is under way that will dramatically affect the delivery of home entertainment. Consumers will soon have hundreds of viewing options from which to choose because of advances in digital compression technologies and the associated reduction in costs accompanying each advance. Because of the increased number of channels more channels will be allocated for pay-per-view (PPV). The increased number of PPV channels will mean video service providers (VSP), also known as PPV providers or system operators, can provide a greater number of movies and more start times, ultimately changing the way many consumers purchase and view movies in their homes. Already, market research experts are predicting that the pay-per-view business will rival today's videocassette rental and sell-through business within 3–5 years.

Even with such a positive outlook for the future of PPV, the full benefits to the consumer of PPV programming may be delayed unless new digital video networks can protect PPV program copyrights. Rights owners are concerned that when digital programming is delivered to the home any digital set-top box will be able to produce a commercial quality video when recorded by a consumer VCR.

SUMMARY OF THE INVENTION

In this new world of direct-to-home video programming, video service providers will be called upon to protect PPV programming against unauthorized copying. They will be obligated to develop and manage the headend (cable) or uplink (satellite) systems which monitor, control, track, and report the application of copy protection on each pay-per-view video program. To this end, the present invention provides copy protection management framework which meets these needs while complementing the more technically detailed copy protection management strategy for video service providers. This framework serves to integrate all components of copy protection delivery in a digital network, and is designed to fit the diverse needs of DBS, Telco, and Cable operators while meeting the requirements of rights owners for a robust and secure environment in which to deliver copy protected PPV programming.

The value of PPV copy protection is maximized when the appropriate control and tracking systems are in place at the video service provider's control and billing centers. These control and tracking systems are best specified during the design phase of the digital signal material delivery system. At a minimum, the following system components are required:

- Copy protection-capable set-top boxes
- Capability to deliver programmable copy protection configuration
- Capability to deliver real time on/off/mode command
- Transaction/billing reporting systems/programs

A control and tracking system in accordance with the invention, for providing copy protection for a typical digital delivery system can be best understood through a short case study which begins when a consumer, that is a subscriber, receives a new set-top box. Each set-top box includes a copy protection capable digital-to-analog encoder chip. When the set-top box is initially powered on, the encoder chip is remotely programmed via a video service provider with the desired copy protection configuration. Thus the video service provider's system management software (SMS), also termed hereinafter as system control software (SCS), has the ability to store and track the designated configuration. The configuration information applies to all copy protected programming and is updated only when a video service provider is informed of a change in the process or when a set-top box is initialized.

The copy protection status or option of each program is contained in the video service provider's system control

software database. There are several potential copy protection status options. For example, a first option is for copy protection which allows for viewing only at a PPV transaction fee. A second option is for copy protection which allows for taping at a higher transaction fee. A third option is for non-protected program material for which no copy protection is required (for example, broadcast television).

When the consumer selects a viewing choice via an electronic program guide, a correct menu of options is displayed. Once a PPV program is selected by the consumer, the correct copy protection status is applied as determined by the consumer's chosen option and scheduling software of the system control software database. Either the headend/uplink facility's control software or software at the set-top box can determine and send the appropriate on/off/mode command to the copy protection capable digital-to-analog chip of previous mention.

The headend/uplink software communicates the on/off/mode command to the set-top box to correctly set the copy protection for a particular program. The system scheduling software has the capability to prevent copy protection from being applied to any type of program other than PPV programming since copy protection is licensed only for use on PPV programming. After a PPV program is viewed by a consumer, the set-top box is able to communicate to a billing subsystem of the system control software all relevant transaction data. From this data the billing subsystem is able to add this information to copy protection activity reports. These reports contain information such as the number of purchases, retail price, and copy protection usage fees owed to a licensor.

The copy protection process is applied to the analog video signal just prior to its exiting the consumer's set-top box. The application of the copy protection process is controlled and managed by system control/access software of the system control software that resides in the video service provider's operations control and billing center.

All set-top boxes in the network need to contain copy protection circuitry. If a set-top box does not have copy protection capability then the video service provider is able to identify those set-top boxes and deny them copy protected PPV programming.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram depicting a summary of the functions of the present invention.

FIG. 2 is a block diagram depicting a typical digital set top box/decoder of the present invention.

FIG. 3 is a block diagram illustrating an example of the circuitry and architecture of the set-top box of FIG. 2 in further detail.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The basic copy protection which is controlled and tracked in accordance with the present invention, is the subject of numerous patents and co-pending applications. The PPV copy protection process works by exploiting the differences between the way television (TV) sets and VCRs respond to video signals. The two components of the anticopy process are known as the automatic gain control (AGC) and Colorstripe™ processes. The purpose of these two separate components or processes is to modify the video signal in a manner which has no effect on a TV set but which inhibits a recording VCR from making a watchable copy.

The combination of the AGC based anticopy process and the Colorstripe™ technology developed specifically for PPV applications results in an overall effectiveness rating of more than 95%. This means that over 95% of unauthorized copies will be either unwatchable or have substantially reduced entertainment value.

Security is also a major factor in the operational effectiveness of PPV copy protection. Security is a measure of the difficulty in bypassing or defeating the anticopy process. Ideally the system is completely undefeatable, but as a practical matter the copy protection system needs to be secure enough to thwart attempted breaches by typical consumers, including reasonably sophisticated consumers. The security system is successful if the vast majority of consumers are prevented from taping PPV programs in the home.

Both video service providers (VSPs), that is, PPV providers, and rights owners benefit when current movie programming is offered to consumers at the same time or shortly after these movies are available on videocassette. Subscribers benefit as well since this scenario provides them with more choices and added convenience.

As digital PPV programming generates increasing revenue for rights owners and becomes a viable viewing option to prerecorded videocassettes, video service providers will be called upon to copy protect PPV programming so that the videocassette rental and videocassette sell-through businesses are not compromised. Rights owners also will require video service providers to monitor, control, track, and report the application of copy protection on each video program for billing purposes.

Copy protection has emerged as a key element in the delivery of PPV programming via digital signal delivery networks. The aggregate system implications of copy protection are very manageable, but only when designed as a part of the overall digital delivery system architecture.

The description of the present invention is intended to apply to systems where one or more video service providers are, or will be in the future, connected to a pay-per-view (PPV) service. The PPV service can be either a video-on-demand (VOD) format, or a near video-on-demand (NVOD) format and digital delivery network, and where set-top boxes (STBs) from multiple manufacturers may be connected to the network. It is assumed that one class of technology will be deployed initially [such as Direct Broadcast Satellite (DBS), Multi-point Microwave Distribution System (MMDS), telephone line or Hybrid-Fiber Coax (HFC)] to be followed by another class of technology at some future date. Although a different technology may arise, it is intended that the invention is applicable to use with multiple platforms and technologies.

FIG. 1 illustrates a control and tracking method and system for enabling and controlling the application of copy protection of video signals and the like via digital video networks. Station 1 represents the issuance of instructions to video service providers by program rights holders who hold the copyrights, for the application by the providers of copy protection to the programs which are protected by per-per-view (PPV) or pay-to-tape (PTT) requirements.

Station 2 depicts a control and billing center of the licensed video service providers who supply copy protection control software for the respective protected programs being broadcast, to generate the commands required to activate, control and reconfigure the copy protection process for each specific PPV/PTT program offering. Although a single provider is depicted, it is understood that station 2 represents any plurality of video service providers each with their respective proprietary control and tracking (billing) software, in accordance with the present invention.

Station 3 represents the procedure of transmitting the particular copy protection command codes of the respective providers, for the PPV/PTT program offerings, via the typical broadcasting networks. Such transmissions may be made by satellite, by microwave, by phone line or by cable transmission systems as depicted.

Station 4 represents the subscriber's home, or other receiving facility, and includes a set-top box 10 for each of a multitude of subscribers. Each set-top box contains copy protection circuitry including a digital color encoder integrated chip (IC), which is adapted to apply selected anticopy waveforms to the analog or digital video signal which is supplied therefrom to a television set or monitor. The receiving facility is further described in FIG. 2.

Station 5 represents the procedure whereby data identifying each PPV or PTT transaction, including copy protection usage, is sent by the set-top box 10 back through the transmission networks of station 3, generally to the respective video service provider's control and billing (tracking) center. The center includes billing procedures which are a subset of the system control software and which process the return transaction data to provide for billing the subscriber for the PPV or PTT transaction usage.

Station 6 represents the procedure whereby each of the licensed video service providers report the copy protection usage to the program rights holder, whereby the provider pays the copy protection fees to the rights holder, i.e., the licensor.

FIG. 2 illustrates in further detail the subscriber's facility, station 4 of FIG. 1, receiving the digital, and usually compressed, pay-per-view transmissions from the broadcasting networks depicted as station 3 of FIG. 1. The compressed digital video signal, or the like, is supplied to the respective set-top box 10 of a multitude of set-top boxes, wherein each box includes conventional circuits for converting and decoding the digital compressed video signal to an analog (baseband) video signal. The set-top box 10 also includes a digital color encoder IC 20 of previous mention which contains copy protection circuitry for applying the selected copy protection waveforms to the analog (or digital) video signal, namely, the programs which are being protected. In this example, the copy protected analog baseband video is supplied by the set-top box to a TV set 22 where the pay-per-view protected program clearly is displayed for viewing if the subscriber is authorized to view the program. If the subscriber is not authorized for a particular PPV protected program, the corresponding picture is modified so as to be un-viewable.

In the event a subscriber records the PPV protected program via a VCR 24 to obtain a taped copy 26 without authorization, the unauthorized copy will be degraded to the degree that it is un-watchable, as depicted by a TV set 28. However, if the subscriber subscribes to a pay-to-tape transaction and to the required higher PTT transaction fee, then the copy is authorized and the resulting taped copy would readily be watchable.

Referring to FIG. 3, there is illustrated in further detail an architecture of the set-top box(es) 10 of FIGS. 1, 2. Upon power up of the set-top box 10 the configuration bits stored in flash memory 48 are read and written into the appropriate CP control registers 52 in the NTSC/PAL encoder 20. When the compressed digital video signal, including the copy protection control commands of previous and following discussion, are supplied by the delivery network of previous mention (satellite, HFC, MMDS, phone line) to a demodulator circuit 32, as depicted by an input lead 30. The demodulated video/audio and control signals are supplied to a demultiplexer circuit 34 where the video/audio signals are separated into respective channels and supplied to an MPEG-2 decoder and digital decompression circuit 36. The copy protection control commands are supplied from the demultiplexer 34 to a conditional access system module 38. The commands are supplied to a microprocessor in a CPU 40. The CPU processes information located in memory that is associated with the Electronic Program Guide (EPG) 46 or runs the copy protection application software 44 residing in memory 42 to deliver the activation command to the NTSC/PAL encoder 20. The EPG may also have data which is used to determine if copy protection should be activated. There are additional methods that may be employed to activate copy protection.

In response to the control commands, the CPU 40 supplies control signals to the NTSC/PAL encoder IC 20 of previous mention, FIG. 2. The encoder IC 20 includes copy protection control registers 50, 52 for receiving the mode bits and configuration control bits respectively, of previous and following discussion. The configuration bits 52 determine the form of the copy protection (i.e., where the Pseudo Sync and AGC pulses will be located or positions of the colorstripe lines etc.) The on/off/mode byte 50 determines which components of the copy protection process will be activated. See table 1 below. The encoder IC 20 also receives decompressed video from the MPEG-2 decoder and digital decompression circuit 36. Encoder IC 20 outputs a RF signal, a composite video signal and/or an S-video signal via video leads 54. The decompressed audio signal is supplied from the circuit 36 to an audio processing circuit 56 which, in turn, outputs left and right channel stereo signals and/or an AC-3 signal on audio leads 58.

In accordance with the invention, the set-top box needs to satisfy certain requirements to insure that the copy protection process is correctly generated, controlled and tracked. Control and tracking of the copy protection process usage takes place at the VSP's control and billing center, station 2 of FIG. 1. This in turn requires that certain capabilities exist which involve the set-top box, the system control and the billing systems and programs in order to satisfy these requirements.

There follows a description of the requirements which ensure that the copy protection process or technique is correctly activated and controlled and its usage tracked. It is expected that if non-compliant set-top box hardware is attached to the digital delivery network, that each licensed service provider will be able to identify such hardware as non-compliant and will withhold copy protected programs from the respective subscriber.

Implementation of these control requirements over the network (i.e. control of the anticopy process from the program origination control and billing center) requires knowledge of the set-top box control system and process, the application program interfaces (API) present at the box and the dialog between it and the integrated circuit (IC) which incorporates the copy protection apparatus.

Copy protection control software (CPCS) is a software module or set of software modules that reside in the service provider's system control software (SCS). It provides a system operator (that is, the service provider) with an interface to manage the necessary attributes of the pay-per-view copy protection in accordance with the present invention.

For security reasons there needs to be the capability to control access to the CPCS from the system control soft-

ware. This restriction is designed to limit access to the CPCS for control of the copy protection process. The operating system supporting the SCS is generally the first level of security. Every employee is required to enter a login account and password. Without these an employee is denied access. The employee's account specifies the respective privileges. A system administrator of the service provider is responsible for the assignment of the employee's privileges.

Thus, every executable file residing on the host which is capable of modifying the operational status of the copy protection process has permissions restricted to authorized personnel. Without the proper permissions, the personnel are unable to run the executable software.

The CPCS is the portion of the video service provider's software control where the decision to apply the options of pay-per-view and pay-to-tape are applied on a program-by-program basis.

There is access control to the CPCS either through password control or the assignment/denial of privileges through software. If password control is the selected method then once the correct initial password is entered, CPCS forces the selection of a new password for future access to CPCS. In this way the service provider can limit access to CPCS to those employees who carry the authority to modify the copy protection database. The password is valid for a reasonable amount of time before it expires and selection of a new password is required.

Additionally there is an access control to a subsystem within the CPCS that allows the modification of selected bits which define the configuration control and mode, and thus determine the characteristics, of the copy protection process. Any unauthorized changes to these bits can result in severe playability and effectiveness problems. In order to maximize the security of the system the video service provider needs to have a short list of personnel who are authorized to change these bits.

A mode control group controls access to the mode bits. This group has the ability to change the contents of the mode byte(s) which is sent with each PPV program to activate or deactivate the copy protection process. The membership of this group is controlled by the system administrator. The number of the service provider's personnel allowed in this group is kept to a minimum.

Similarly, a configuration control group controls access to the configuration bits. This group has the ability to change the contents of the configuration bits which define the copy protection process. These are the bits that are sent periodically to every set-top box to assure that all boxes are using the correct version of the process. The number of the service provider's personnel allowed in this group also is kept to a minimum.

Each password described below should be at least eight (8) alpha-numeric characters in length. The system administrator is responsible for defining and distributing the current password to the authorized personnel. Each password described below should have a life of no more than four months before the system administrator changes the password.

Password access to the software that applies or removes the copy protection process on a program-by-program basis is designed to query mode or configuration control group authorized personnel for an authorization password to ensure that they are a member. If the authorized personnel correctly enter the password they will be allowed to apply or remove the copy protection for a particular PPV or series of PPV events. Conversely, if authorized personnel fail to enter the password they must be denied access to that portion of the database. It is the system administrator's responsibility to ensure that only authorized personnel know the password for either the mode or configuration control. An authorized personnel will be given three attempts to login before a message is generated for the system administrator that an unauthorized request to modify the application or remove the copy protection has been made.

Alternative proposals for accessing CPCS and controlling access to the mode and configuration of the copy protection process may be developed by one skilled in the art.

The CPCS will perform the following functions: Copy protection on/off and mode control; copy protection validation; functionally unlocking copy protection capability in a set-top box; and copy protection process configuration reprogramming.

The copy protection process which is incorporated in the set-top box is controlled by the CPCS at the licensed video service provider's control and billing central location. The need to invoke copy protection on an individual program forms part of a descriptor for each program. A default for copy protection within the descriptor needs to be turned off (i.e., no copy protection).

Steps need to be taken to prevent copy protection being applied to non-PPV program channels, since copy protection can be licensed only for PPV programming. If the system control software automatically verifies that a program is designated for PPV use, this requirement may be automated. Similarly, access to CPCS may be automatically denied for non-PPV programming. If such an automatic verification is not made, a warning notice is generated when CPCS is accessed to change the copy protection status of a program. This notice needs to be displayed until a specific keyboard entry is made to acknowledge the warning.

In the case of MPEG signals, the MPEG copyright header bits on their own are not sufficient to activate copy protection in the set-top box. The following reasons are the basis for not allowing the MPEG header bits to be used as the sole control of the copy protection process. An application routine is required in order to (a) differentiate between digital-to-digital and digital-to-analog copy protection conditions, (b) provide sufficient control capacity to set the copy protection operating mode, and (c) facilitate access to the copy protection system only by licensed video service providers.

It is preferred that the anticopy process on/off control is achieved by setting all the individual parameter on/off and mode control bits rather than a master on/off control. This requires that the N0 (N-zero) bits in the control bit listing be set as required. Depending on the individual system, this will require the control of from 5 to 8 bits.

The delivery of the mode byte to the set-top box to activate or deactivate the copy protection process may be accomplished in several ways. Each method has its positive aspects as well as its negative aspects. When selecting a mechanism to control the copy protection technology, a service provider selects one of the following means or may develop an entirely new means.

One method may be for the mode byte to be delivered via the conditional access system via the entitlement control message (ECM). Another method might be to include the mode byte in a private data field in the MPEG transport data stream.

Another method may deliver the mode byte in a user defined section of the electronic program guide (EPG) that is not identified in released documentation as controlling copy protection. This method also requires some additional

security to keep the memory location of the mode byte from being accessed for unauthorized changes and the setting of a return flag that indicates the actual status of the mode byte when transmitted to the NTSC encoder.

Another method may be a combination of the conditional access ECM and EPG. The transport of the mode byte in the EPG could be combined with two bits within the ECM. To activate the copy protection technology then it would be an or operation between the ECM bits and the EPG bits. If either is set, the copy protection technology, both ECM and EPG would have to indicate that deactivation is necessary.

When a copy protected PPV program is viewed, part of the information that will need to be tracked will be the actual setting of the mode byte. In this way both the copy protection process and the service provider will have a means to discover if copy protection has been circumvented in the set-top box. The return flag may be a simple bit set to 'true' to indicate that the copy protection process was correctly activated and 'false' if it was incorrectly activated. It is required that the mode byte be sent to the NTSC encoder on a periodic basis. The frequency of the transmission is on the order of once every minute.

Setting the operating mode of the copy protection process requires independent activation of the three component parts of the copy protection process (pulses within the vertical blanking interval, pulses at end of field, colorburst phase modification) and up to 5 additional mode set parameters using N0 bits as indicated above.

Access to copy protection at the set-top box by the video service provider needs to be restricted to authorized providers. This should not to be confused with access to the CPCS as defined earlier. It follows that each system operator or video service provider is required to procure the means (i.e., keys/codes, etc.) to activate the copy protection system control software on a program-by-program basis. When a service provider obtains the means to activate copy protection, the provider will gain access to the copy protection process at the set-top box. The copy protection process (i.e. on/off/mode or reprogramming commands) at the set-top box needs to have controlled access such that only authorized providers can issue valid commands to the box. The set-top box needs to reject commands for the copy protection process from unauthorized video service providers.

Set-top boxes such as depicted in FIGS. **1**, **2**, may be shipped by the manufacturer with the copy protection capability installed, but functionally locked. This means that the set-top box will not respond to any copy protection control codes. However, the set-top box will be unlocked (i.e. enabled) by a message initiated via the CPCS or SCS and sent through the system by a licensed video service provider. This message may be sent as part of the log-on routine when a subscriber accesses a provider. This message need only be acted upon once by the set-top box during the lifetime of the box. Only authorized video service providers are provided with the unlocking message data.

The copy protection unlock message consists of at least 8 bytes. The set-top boxes are manufactured with an appropriate unlock message code. This code is provided by the set-top box manufacturer only to a copy protection licensor, who in turn provides the code to licensed video service providers. The copy protection unlock message is different for each set-top box manufacturer, but is the same for all boxes made by that manufacturer.

Alternative proposals on the methodology to enable the copy protection process in the set-top box will be apparent to those skilled in the art.

To ensure that over the life of the set-top box the copy protection process provides the maximum effectiveness with VCRs and compatibility with TV sets, the copy protection system needs to be upgradeable on a system-wide basis by means of commands initiated by the CPCS. This will result in new process configuration data being transmitted. In response, the set-top box processes the data to reconfigure the adjustable parameters of the copy protection process. The set-top box may be placed in a "diagnostics" mode for this feature implementation, or the configuration data may be sent and acted on by the box on a routine basis as part of the program description data or log-on routine.

However, it is recommended that the entitlement control message (ECM) be used. The ECM is embedded in the conditional access system.

In one version, configuration data of 108 bits is provided to accommodate the reconfiguration data, however, 108 bits does not fall on a byte boundary. Therefore, it is recommended that 112 be sent with a pad **0**. The data is presented to the service provider in the form of hexadecimal numbers for entry into the CPCS. The 112 bits thus are entered as a string of 28 hexadecimal numbers.

In another version, configuration data of 132 bits is provided to accommodate the reconfiguration data, however, 132 bits does not fall on a byte boundary. Thus, it is recommended that 136 be sent with a pad **0**. The data is presented to the provider in the form of hexadecimal numbers for entry into the CPCS. The 136 bits thus are entered as a string of 34 hexadecimal numbers.

It is possible to verify the current configuration stored by the CPCS by accessing the current contents of the configuration bits presented as the correct number hexadecimal characters. An alpha-numeric password of at least 8 bytes is required to gain access to change the programming data within CPCS. This password is separate from the password which allows access to CPCS. The service provider has the option of receiving the 'C' source code of an executable file to which to pass parameters.

The following warning notice is presented on the screen of the operational control and billing center of a provider after entering the correct password:

WARNING

Changing this copy protection configuration data without the written authorization carries the serious risk of problems with the performance of the copy protection system and degraded picture quality.

This warning notice is displayed until a specific keyboard entry is made to acknowledge the warning.

By way of example only, Table 1 illustrates a mode control bit listing which defines the corresponding bit pattern or command, which provides the routine on/off and mode selection functions when transmitted to the set-top boxes via the delivery networks. The configuration control bit listing is generally equivalent to that of the mode control, though relatively longer since it controls considerably more control and reprogramming functions.

TABLE 1

Mode Control Bit Listing
Routine On/Off and Mode Selection

NO	On/off and mode control; 8 bits		
NO[7]	Reserved		CPC0[3]
NO[6]	Pay-to-tape allowed/prohibited	(Allowed = 1, Default = 0)	CPC0[2]
NO[5]	VBI pulses On/Off (VBIP)	(ON = 1)	CPC0[1]
NO[4]	End of Field Back Porch Pulses on/off (EOFP)	(ON = 1)	CPC0[0]
NO[3]	Colorstripe process On/Off (CSP)	(ON = 1)	CPC1[3]
NO[2]	AGC pulse normal (amplitude cycling)/static mode select (AGCY)	(Cycling = Default = 1)	CPC1[2]
NO[1]	H-sync amplitude reduction On/Off (HAMP)	(ON = 1)	CPC1[1]
NO[0]	V-sync amplitude reduction On/Off (VAMP)	(ON = 1)	CPC1[0]

The pay-per-view transaction information is collected by each video service provider for each subscriber so that monthly copy protection activity reports required for royalty payments and other fees may be generated. The reports include information regarding the number of subscribers accessing each copy protected program, with subtotals of the copy protection status or options selected by respective subscribers. The reports further include information sorted by PPV title, PPV program supplier, copy protection activation status requested by the subscriber, and by set-top box model code. The reports are provided by the report generating software of previous mention at the video service provider centers.

The activity report includes a manufacturer and model type descriptor code in the transaction acknowledgment between the set-top box and the control and billing system when a PPV purchase transaction is reported to the provider.

The CPCS and the set-top box are capable of applying and reporting anticopy usage according to the following conditions. The overall system allows the subscriber's copy protection to be turned off at the box only as permitted by the PPV program rights holder.

(a) PPV program rights holder permits viewing only:

The pay-to-tape mode is prohibited (off). All STBs output copy protected waveform only. I.e., the copy protection waveform unconditionally appears on the set-top box analog video output signal.

This is reported to the billing system as a "pay-per-view" copy protected transaction.

(b) PPV program rights holder permits viewing and recording:

The pay-to-tape mode bit is set for pay-to-tape permitted (on). Under this option, when the subscriber selects the "pay-to-tape" option, the copy protection process is turned "off" in the STB to allow the PPV program to be recorded (taped) for a higher transaction fee than for "viewing only." I.e., the copy protection waveform will not be present on the STB analog video output signal.

This is reported to the billing system as a "pay-to-tape" copy protected transaction.

The following Table 2 provides a summary of the control options and includes additional information.

TABLE 2

Pay-per-view and Pay-to-tape Control Options
for Pay-per-view Programs

Program Descriptor of PPV Program	Consumer Request (Pay-per-view or Pay-to-tape)	Result
Copy protection NOT required	N/A	ACP off
Copy protection REQUIRED Taping NOT permitted	Pay-per-view	ACP will be ON. Pay-per-view transaction cost incurred by consumer.
Copy protection REQUIRED Taping NOT permitted	Pay-to-tape	Requested option not available. ACP will be ON. Pay-per-view transaction cost incurred by consumer.
Copy protection REQUIRED Taping permitted (at higher transaction cost)	Pay-per-view	ACP will be turned ON by STB control system. Pay-per-view transaction cost incurred by consumer.
Copy protection REQUIRED Taping permitted (at higher transaction cost)	Pay-to-tape	ACP will be turned OFF by STB control system. Pay-to-tape transaction cost incurred by consumer.

It is to be understood that various terms employed in the description herein are interchangeable. For example, a "video service provider" also is known as a pay-per-view (PPV) provider or a system operator, and the "system management software" preferably is referred to as the system control software. Likewise, the "control and billing centers" of the PPV providers represented by station 2 (and generally station 5) also may be referred to as operations control/tracking centers, program origination/termination centers, headend (cable) uplink (satellite) control centers, etc. A licensed PPV provider facility supplies the necessary control instructions to associated software and/or circuitry in a set-top box to allow a respective subscriber access to program material to which he or she is entitled, and also receives at designated times of the week, month, etc., the usage data automatically returned by the set-top box. A billing and license fees software subset of the system control software then enables each PPV provider to bill the subscribers and to report and pay the attendant licensing fees to the rights holders, etc.

Accordingly, the above description of the invention is illustrative and not limiting. Further modifications will be apparent to one of ordinary skill in the art in light of this disclosure. For example, although the invention is described herein relative to a video signal, and primarily an analog video signal, it is to be understood that the invention concepts may be applied to other signals with properties equivalent to a video signal where copy protection is desired. Likewise, the invention is applicable to the copy protection of digital as well as analog signal materials, such as those disclosed in the U.S. Pat. No. 5,315,448 of previous mention. Further, although a specific example of a code word is disclosed herein for enabling the copy protection process via the set-top box, other combinations and numbers of bits may be employed. In addition, a selected portion of the control software for effecting the copy protection process may reside in the set-top box in the form of an insertable "smart" card, wherein for example the smart card contains the data concerning the subscriber's options and privileges.

Thus, the scope of the invention is defined by the following claims and their equivalents.

What is claimed is:

1. A method of providing copy protection of signal material transmitted via digital delivery networks to a consumer's set-top box, to prevent copying and/or subsequent viewing of a recorded copy of the signal material, comprising:

supplying copy protection controls indicative of desired copy protection for the signal material;

storing a copy protection configuration corresponding to the desired copy protection in the set-top box;

transmitting commands derived from and in response to the copy protection controls which activate the copy protection configuration for the signal material; and

applying the copy protection configuration to the signal material in response to the commands to prevent the subsequent viewing of the recorded copy of the copy protected signal material while allowing viewing of the original signal material as via a television set;

wherein the step of supplying includes;

establishing requirements for activating and controlling a process which enables the application of said copy protection configuration and which reports the corresponding usage thereof; and

providing copy protection control software in response to the requirements, which software provides said copy protection controls to activate and control the application of the copy protection configuration and the usage reports.

2. The method of claim 1 wherein the step of establishing includes:

establishing requirements which differentiate between digital-to-digital and digital-to-analog copy protection conditions, which determine a copy protection process operating mode and configuration, and which ensure that there is only authorized access to the copy protection process.

3. The method of claim 1 wherein the step of providing includes:

generating commands in the form of bit patterns in response to the copy protection control software; and

said commands including a first mode bit pattern which enables real time on/off/mode control for selecting components of the copy protection configuration, and a second configuration bit pattern which determines a programmable copy protection configuration.

4. The method of claim 3 including:

receiving the transmitted first and second bit patterns to activate the copy protection and to control and reconfigure the copy protection process respectively in response thereto; and wherein the anticopy waveforms are applied to the signal material to provide the copy protection.

5. The method of claim 1 including:

limiting access to the steps of establishing and providing to prevent unauthorized access to the application of the copy protection process or to the copy protection control software which activates and controls the process.

6. The method of claim 1 wherein the step of applying includes:

storing the copy protection controls in memory at a consumer's set-top box; and

storing control data in memory at a signal material receiving set-top box, which stored control data is responsive to the transmitted commands to activate, control and reconfigure the stored copy protection configuration.

7. The method of claim 1 including:

collecting periodic copy protection activity information including copy protection activation status such as the number of pay-per-view and pay-to-tape signal material events watched.

8. The method of claim 7 further including generating reports which include the number of accessing receiving set-top boxes, the rights holder of the signal material events, the number of total events watched, and corresponding billing information.

9. The method of claim 1 wherein the step of applying includes:

modifying a selected synchronizing signal in a corresponding blanking interval of a television line in response to said commands to degrade a subsequent decoding of the synchronizing signal in the event that a recording is made of the corresponding copy protected signal material.

10. The method of claim 1 wherein the signal material is a video analog or digital signal.

11. A method of providing copy protection of signal material transmitted via digital delivery networks to a consumer's set-top box, to prevent copying and/or subsequent viewing of a recorded copy of the signal material, comprising:

supplying copy protection controls indicative of desired copy protection for the signal material;

storing a copy protection configuration corresponding to the desired copy protection in the set-top box;

transmitting commands derived from and in response to the copy protection controls which activate the copy protection configuration for the signal material; and

applying the copy protection configuration to the signal material in response to the commands to prevent the subsequent viewing of the recorded copy of the copy protected signal material while allowing viewing of the original signal material as via a television set;

wherein the step of supplying includes;

developing copy protection control software which describes control signals for applying the copy protection process to the signal material and for returning to a service provider usage data indicative of the signal material selected at the consumer's set-top box;

generating mode and configuration control bit patterns in response to the copy protection control software; and

transmitting said control bit patterns to the consumer's set-top box when the consumer joins the delivery network and thereafter on a prescribed routine basis.

12. The method of claim 11 including:

storing in the set-top box the configuration control bit pattern which determines the form of the copy protection process; and

enabling the stored configuration control bit pattern in response to the transmitted mode control bit pattern to selectively activate and/or modify the configuration of the copy protection process.

13. The method of claim 12 including:

modifying the configuration control bit pattern commensurate with a desired change in the form of the copy protection process; and

transmitting the modified configuration control bit pattern to the set-top box to effect the change in the copy protection process.

14. The method of claim 12 including:

storing consumer information in the set-top box which is indicative of copying options desired by the consumer; and

comparing the mode control bit pattern to the stored consumer's information in the set-top box when a selection of the signal material is made to determine if the consumer is authorized to view only and/or to copy the material.

15. The method of claim 11 wherein the signal material is a pay-per-view (PPV) or pay-to-tape (PTT) signal and the step of supplying includes:

establishing requirements for activating and controlling the PPV and PTT copy protection process and for reporting the corresponding usage activity of the process to the service provider; and

providing copy protection control software m response to the requirements, which software provides said control bit patterns to activate, control and modify the PPV and PTT copy protection process.

16. The method of claim 15 including:

providing limited access to the steps of establishing and providing to prevent unauthorized access of service provider personnel to the control of the copy protection process or to the copy protection control software.

17. The method of claim 15 wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

18. The method of claim 15 wherein the step of applying includes:

modifying a selected synchronizing signal in a corresponding blanking interval of a television line in response to said control bit patterns to degrade any subsequent decoding of the synchronizing signal when an unauthorized attempt is made to view or copy the pay-per-view signal.

19. A method of providing copy protection of signal material transmitted via digital delivery networks to a consumer's set-top box, to prevent copying and/or subsequent viewing of a recorded copy of the signal material, comprising:

supplying copy protection controls indicative of desired copy protection for the signal material;

storing a copy protection configuration corresponding to the desired copy protection in the set-top box;

transmitting commands derived from and in response to the copy protection controls which activate the copy protection configuration for the signal material;

applying the copy protection configuration to the signal material in response to the commands to prevent the subsequent viewing of the recorded copy of the copy protected signal material while allowing viewing of the original signal material as via a television set;

receiving and writing a mode control bit pattern in the set-top boxes; and

wherein the stored copy protection configuration responds to the transmitted mode control bit pattern to activate, control and modify the copy protection process as defined by the mode control bit pattern.

20. The method of claim 19 wherein the set-top box is functionally locked including:

downloading via the service provider a selected bit pattern or software adapted to functionally unlock the set-top box.

21. A system for controlling copy protection of proprietary signal material transmitted via digital delivery networks, wherein a service provider enables a copy protection process which prevents unauthorized copying and/or subsequent viewing of the recorded signal material by consumers even when the original signal material is watchable, the system comprising:

a control/billing center for supplying copy protection control signals as directed by the service provider;

wherein said copy protection control signals define a first mode command which enables real time mode control as well as on/off control of selected components of the copy protection process, and a second configuration bit pattern command which determines a programmable operating configuration of the copy protection process;

a transmitter for transmitting the signal material, the first mode command and the second configuration bit pattern command in response to the copy protection control signals to selectively control the copy protection process; and

a device located with each consumer for applying said programmable operating configuration of the copy protection process to the signal material in response to the transmitted first and second commands to prevent copying and/or subsequent viewing of the recorded signal material while allowing watching of the signal material.

22. The system of claim 21 wherein the copy protection control signals include an access password for identifying that a service provider's authorized personnel have access to and control of the copy protection process.

23. The system of claim 21 wherein the device located with each consumer is a set-top box having an encoder containing a copy protection circuit adapted to add anticopy signals in the form of said programmable operating configuration to the signal material in response to the first mode command signal.

24. The system of claim 23 wherein:

the set-top box includes memory for storing the configuration bit pattern of the second command separately from the first mode command; and

the encoder includes a buffer for receiving the mode command and the configuration bit pattern and circuitry for controlling the activation and configuration of the copy protection process in response to the first mode command with the configuration being determined by the configuration bit pattern.

25. The system of claim 23 wherein the set-top box sends usage data back to the service provider's control/billing center, the usage data being used by the service provider to bill the consumers and to provide a report of the usage and corresponding license fees.

26. The system of claim 21 wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

27. The system of claim 21 wherein the control/billing center includes:

instructional information for establishing requirements for activating and controlling the copy protection process and for reporting the copy protection activity; and

wherein the service provider supplies copy protection control software corresponding to said requirements and said copy protection control signals in response to the copy protection control software.

28. A method for providing copy protection of signal material transmitted via digital delivery networks, to prevent copying and/or subsequent viewing of the recorded signal material while allowing viewing of the original signal material, comprising:

generating at least first and second copy protection commands, wherein the second command comprises a changeable configuration bit pattern indicative of a corresponding programmable copy protection configuration for application to the signal material;

transmitting the signal material and the first and second copy protection commands to a plurality of remote devices coupled to the networks and;

in response to the copy protection commands, activating the configuration bit pattern defining the programmable copy protection configuration for the signal material in one or more remote device to prevent said copying and/or subsequent viewing of the recorded signal material while allowing viewing of the original signal material.

29. The method of claim 28, including:

storing the changeable configuration bit pattern in respective remote devices; and

wherein the configuration bit pattern is recovered from storage in response to the first copy protection command to activate the copy protection for the signal material thereby modifying the signal material such that a copy thereof is un-viewable, is viewable but un-copiable or to cause the remote devices to stop outputting the signal material.

30. The method of claim 28, wherein the step of generating comprises:

establishing requirements for activating and controlling the copy protection process and reporting corresponding usage thereof;

providing copy protection software in response to the selected requirements; and

generating the first and second copy protection commands in response to the copy protection software to update, activate and control the programmable copy protection configuration and usage reports.

31. The method of claim 30, wherein the step of establishing includes establishing requirements to differentiate between digital-to-digital and digital-to-analog copy protection conditions, to determine a copy protection process operating mode for the first copy protection command and the configuration bit pattern of the second command, and to ensure only authorized access to the copy protection process is allowed.

32. The method of claim 30, wherein the first and second copy protection commands include a first bit pattern for on/off/mode control and a second bit pattern which defines the programmable copy protection configuration.

33. The method of claim 32, wherein authorized access to the copy protection process and the copy protection software is limited to selected employees.

34. The method of claim 30 wherein the usage reports are based on pay-per-view and pay-to-tape activities of the signal material.

35. The method of claim 34 further including the step of generating reports having information on identity of rights holder of the signal material, number of times the remote devices are accessed, number of events watched, and corresponding billing information.

36. The method of claim 28, wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

37. A system for controlling copy protection of signal material transmitted via digital delivery networks coupled to a plurality of remote devices, wherein a service provider enables a copy protection process which prevents copying and/or subsequent viewing of the recorded signal material even when the original signal material is viewable, the system comprising:

a controlling/billing center for supplying at least first and second copy protection control signals as directed by the service provider;

wherein the second control signal is a configuration bit pattern indicative of a programmable copy protection configuration;

a transmitter for transmitting first and second commands commensurate with the first and second copy protection control signals to determine and control the copy protection process; and

at least one remote device including an encoder coupled to the networks and responsive to the first and second commands for applying the programmable copy protection configuration to the signal material in response to the first command to prevent the copying and/or subsequent viewing of the recorded signal material even when the original signal material is viewable.

38. The system of claim 37, including:

a memory for storing the configuration bit pattern indicative of the programmable copy protection configuration; and

circuitry for recovering the configuration bit pattern from the memory for activating the copy protection for the signal material thereby modifying the signal material such that a copy thereof is unviewable, is viewable but un-copiable or to cause the remote devices to stop outputting the signal material.

39. The system of claim 37, wherein the first and second copy protection control signals comprise:

a first bit pattern for on/off/mode control; and

a second bit pattern which defines the programmable copy protection configuration.

40. The system of claim 39, wherein the copy protection further comprises an access password for ensuring that only authorized access by service provider personnel is allowed to control the copy protection process.

41. The system of claim 39, wherein the remote devices monitor and provide usage data to the controlling/billing center to enable generating usage and associate license fee reports for billing purposes.

42. The system of claim 39, wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

43. A method of providing copy protection of signal material transmitted to remote devices via digital delivery networks to prevent copying and/or subsequent viewing of a recorded signal material, comprising:

receiving copy protection commands at one or more of the remote devices, which commands are indicative of desired copy protection for the signal material and which are transmitted by a control center coupled to the digital delivery networks;

wherein the copy protection commands include a first bit pattern for enabling mode control as well as on/off control of the copy protection, and a programmable second bit pattern for determining the configuration of the copy protection to be applied to the signal material; and

activating the copy protection for the signal material by applying the copy protection configuration determined by the programmable second bit pattern in response to the first bit pattern to prevent unauthorized copying and/or subsequent viewing of the recorded signal material.

44. The method of claim 43, wherein the first bit pattern is compared against information provided by a consumer in the one or more remote devices, which information is indicative of desired viewing and/or copying options to determine whether the consumer is authorized to receive, view and/or copy the signal material.

45. The method of claim 43, wherein the remote devices generate and transmit reports having information on identity of a rights holder of the signal material, number of times the remote devices are accessed, number of events watched, and corresponding billing information, to the control center.

46. The method of claim 43, wherein access to the copy protection commands by personnel in the control center is restricted to prevent unauthorized access.

47. The method of claim 43, wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

48. A device coupled to digital delivery networks for controlling copy protection of signal material transmitted via the digital delivery networks, to prevent copying and/or subsequent viewing of a recorded signal material, the device comprising:

a central processing unit (CPU);

memory coupled to the CPU for storing instructions and information associated with copy protection control commands, the copy protection control commands being indicative of desired copy protection for the signal material and which are transmitted to the device by a control center via the digital delivery networks;

wherein the information associated with the copy protection control commands includes a first mode bit pattern for on/off/mode control which enables real time mode control of selected components of the copy protection process, and a second configuration bit pattern for determining a programmable copy protection configuration of the copy protection process; and

an encoder circuit coupled to the CPU and the memory for receiving the first mode bit pattern and the second configuration bit pattern, wherein the CPU executes the instructions stored in the memory in response to the copy protection control commands to provide commands to the encoder circuit which apply the programmable copy protection configuration to the signal material in response to the first mode bit pattern to prevent the unauthorized copying and/or subsequent viewing of the recorded signal material.

49. The device of claim 48, wherein the CPU compares the first mode bit pattern against information provided by a consumer and stored in the memory which indicates desired viewing and/or copying options to determine whether the consumer is authorized to view and/or copy the signal material.

50. The device of claim 49, wherein the memory further stores information provided by a consumer including the identity of rights holder of the signal material, number of receiving facilities that are accessed, and number of events watched, the device reporting the information provided by the consumer to the control center for billing purposes.

51. The device of claim 48 further comprising a conditional access module coupled to the CPU, the conditional access module preventing unauthorized access by personnel in the control center to the information associated with copy protection commands stored in the memory.

52. The device of claim 48, wherein the signal material is a pay-per-view or pay-to-tape video analog or digital signal.

* * * * *